T · · Com

Personal Security Service

Benutzerhandbuch



Version 5.0

Windows 98/ME/2000/XP

Stand: 09/2004

Hinweis für PSS Softwarepaket mit zeitlich begrenzter Nutzung für 12 Monate. Mit dem beiliegenden Registrierungsschlüssel kann die Software für zwölf Monate aktiviert werden, danach werden die Funktionen automatisch deaktiviert. Die Nutzungszeit beginnt mit der erfolgreichen Installation der Software. Das Ende der Nutzungszeit ist im Programm unter dem Punkt Meine Anmeldung ersichtlich. Vor Ablauf der Nutzungszeit erfolgt ein Hinweis.

Systemvoraussetzungen. Die Personal Security Service Software ist nur unter Windows® 98[1)], Windows® 2000, Windows® ME und Windows® XP lauffähig.
Systemvoraussetzung für AntiVirus und Internet-Schutzschild (minimal):
- Pentium®-II-Prozessor 300 MHz
- Windows® 98/ME: 64 MB Hauptspeicher
- Windows® 2000/XP: 128 MB Hauptspeicher
- Festplattenspeicher während der Installation: 200 MB
- Festplattenspeicher nach der Installation: 130 MB

Systemvoraussetzung für AntiVirus, Internet-Schutzschild, Anti Spam und SurfControl
- Pentium®-II-Prozessor 300 MHz
- Windows® 98/ME: 128 MB Hauptspeicher
- Windows® 2000/XP: 256 MB Hauptspeicher
- Festplattenspeicher während der Installation: 300 MB
- Festplattenspeicher nach der Installation: 210 MB

Server-Versionen werden nicht unterstützt. Eine andere Anti-Virus-, Firewall- oder VPN-Software darf auf dem Rechner nicht installiert sein. Außerdem wird eine Internetverbindung zur Aktualisierung als Wähl- oder Festverbindung mit einer Modemgeschwindigkeit von 56 kbit/s oder schneller benötigt.

Die Nutzung des Registrierungsschlüssels ist jeweils nur auf einem PC und dort nur unter einem Betriebssystem möglich; er ist immer auf dem PC aktiv, auf dem er zuletzt freigeschaltet wurde.

[1)] Die hier genannten Produkt- und Firmennamen sind Marken der jeweiligen Eigentümer.

Inhalt

Über dieses Handbuch **6**
Symbolglossar 7

1. Personal Security Service installieren **8**
1.1 Vor der Installation 8
1.2 Installation von der Personal Security Service CD 9
1.3 Installation von Personal Security Service über das Internet 11
1.4 Wenn Personal Security Service deinstalliert werden muss 13
1.5 Startup-Assistent 14

2. Erste Schritte **18**
2.1 Personal Security Service erstmals verwenden 18
2.2 Vorgehensweise bei Anzeige des Anwendungssteuerungs-Pop-ups 18
2.3 Vorgehensweise bei Anzeige des Fensters vom Dialerschutz 19
2.4 Erstmaliges Verwenden des Programms 21
2.5 Optionen zum Öffnen des Hauptmenüs 23
2.6 Anlegen eines Spam-Ordners in Ihrer E-Mail-Software 26
2.7 Start-Einstellungen für SurfControl 29

3. Statusseite **30**
3.1 Anmeldestatus 31
3.2 Sicherheitsinfos 32

4. Virenschutz **34**
4.1 Virenschutzprofile 36
4.2 Nach Viren scannen 36
4.3 Viren vom Computer entfernen 37
4.4 Vorgehensweise bei Feststellen eines neuen Virus 42
4.5 Erweiterter Virenschutz 43
4.5.1 Echtzeit Scanning 44
4.5.2 E-Mail Scanning 46
4.5.2.1 Scan-Optionen 47
4.5.2.2 E-Mail-Aktionen 47
4.5.2.3 E-Mail Scanning 48
4.5.3 Geplantes Scanning 51
4.5.4 Manuelles Scanning 52
4.6 Schutzeinstellungen zum Ignorieren/Scannen ausgewählter Dateien aktivieren 54

5. Internet-Schutzschild **56**
5.1 Erweiterte Einstellungen 58
5.2 Sicherheitsstufe für den Internet-Schutzschild 59
5.2.1 Ändern der Sicherheitsstufe für den Internet-Schutzschild 59
5.3 Alarmmeldungen vom Internet-Schutzschild 59
5.3.1 Alarmeigenschaften 60
5.3.2 Zuletzt gesendeter Alarm 61
5.4 Anpassen von Internet-Schutzschild-Regeln 62
5.4.1 Erstellen von neuen Internet-Schutzschild-Regeln 63
5.5 Anwendungssteuerung 68
5.5.1 Anwendungseigenschaften 70
5.5.2 Was gilt als sichere Anwendung? 74
5.5.3 Was gilt als unsichere Anwendung? 74
5.5.4 Bestimmte Verbindungen zulassen und alle übrigen ablehnen 75
5.5.5 Bestimmte Verbindungen ablehnen und alle übrigen zulassen 75
5.6 Intrusion Prevention 77
5.7 Dialerschutz 78
5.7.1 Dialerschutz-Protokollfunktion 80
5.7.2 Telefonnummern in der Dialerschutz-Liste anzeigen und bearbeiten 80
5.7.3 Einstellungen 82
5.8 Protokollfunktion 83
5.8.1 Paketprotokollierung 83
5.8.2 Aktionsprotokoll 84
5.8.3 Ändern einer Firewall-Richtlinie, z. B. Ändern der Sicherheitsstufe 84
5.8.4 Öffnen einer eingehenden oder ausgehenden lokalen Verbindung 84
5.8.5 Empfangende Verbindung 85
5.8.6 Eingabe einer dynamischen Regel 85

6. Anti Spam **86**
6.1 Funktionsweise von Anti Spam und Filtermodus 87
6.2 Zugelassene Absender 88
6.2.1 Hinzufügen und Entfernen von Adressen 88
6.2.2 Importieren von Kontakten 89
6.3 Gefilterte Absender 89
6.3.1 Hinzufügen und Entfernen von Adressen 90

7. SurfControl **92**
7.1 Webseitenfilter 93
7.2 Aufgerufene Webseiten 94
7.3 Zugelassene und gesperrte Webseiten 95
7.3.1 Zugelassene Webseiten 95
7.3.2 Gesperrte Webseiten 96
7.4 Passwort für SurfControl 97
7.4.1 Erstellen des Passworts für SurfControl 98

8. Automatische Updates **100**
8.1 Erweiterte Einstellung 102
8.1.1 Verbindung 102
8.1.1.1 Client-Standardprotokoll 102
8.1.1.2 Einrichtung des Polite-Protokolls 103
8.1.1.3 Unterschied Polite-Protokoll und HTTP 104
8.1.1.4 Internetverbindung 104
8.1.1.5 Verbindungspläne 105
8.1.2 Proxy 106
8.1.2.1 HTTP-Proxy-Setup 107
8.1.3 Heruntergeladene Dateien 108

9. Allgemein **110**
9.1 Sicherheitsinfos 110
9.2 Meine Anmeldung 111

10. So schützt Personal Security Service Ihren Computer **112**
10.1 Virenschutz 112
10.2 Internet-Schutzschild 112
10.3 Anti Spam 114
10.4 SurfControl 115
10.5 So schützen Sie sich gegen Viren und andere Malware 117

Häufig gestellte Fragen (FAQ) **118**
PSS Betrieb allgemein 118
Installation 119
Virenschutz 121
Virenscan 122
Dialerschutz-Funktion 123
Internet-Schutzschild 124
Anwendungssteuerung 124
SurfControl 125
Automatische Updates 126
Anti Spam 127

Glossar **128**

Technische Unterstützung **130**

Wartung **132**

Über dieses Handbuch

Dieses Handbuch enthält alle Informationen, die Sie zur Installation und Verwendung von Personal Security Service benötigen.

Kapitel 1: Personal Security Service installieren. Enthält die zur Installation von Personal Security Service erforderlichen Informationen.

Kapitel 2: Erste Schritte. Bietet Informationen zum Zugriff auf Personal Security Service sowie erste Schritte für neue Benutzer bzw. Hinweise für bereits erfahrenere Benutzer.

Kapitel 3: Statusseite. Bietet eine detaillierte Übersicht über Ihre Sicherheitseinstellungen und den Status von Personal Security Service.

Kapitel 4: Virenschutz. Erklärt die Aktivierung bzw. Deaktivierung des Virenschutzes, die Auswahl Ihres Virenschutzprofils sowie die Überwachung nach Erhalt von Virendefinitions-Aktualisierungen.

Kapitel 5: Internet-Schutzschild. Erklärt das Ändern und Bearbeiten von Internet-Schutzprofilen, das Überprüfen der zugelassenen und abgelehnten Verbindungen sowie den Zugriff auf erweiterte Einstellungen.

Kapitel 6: Anti Spam.

Kapitel 7: SurfControl.

Kapitel 8: Automatische Updates. Enthält Informationen zum automatischen Aktualisierungsservice, der für Sie die neuesten Vireninformationen, Software-Versionen und Profilversionen bereitstellt.

Kapitel 9: Allgemein.

Kapitel 10: So schützt Personal Security Service Ihren Computer. Definiert die Gefahren für Ihren Computer und erklärt, wie Personal Security Service Ihren Computer gegen diese Bedrohungen schützt.

Häufig gestellte Fragen (FAQ) – häufig gestellte Fragen (Problemlösungen).

Glossar.

Technische Unterstützung – enthält Kontaktinformationen, wenn Sie Unterstützung benötigen.

Symbolglossar

Die folgenden Symbole werden bei Personal Security Service verwendet:

Symbol	Name	Beschreibung
	Aktiv	Personal Security Service ist aktiviert und funktioniert fehlerfrei.
	Info	Informativer Text zur Unterstützung bei der Verwendung von Personal Security Service.
	Kritische Warnung	Dieses Symbol wird angezeigt, wenn die Virendefinitionen in der letzten Zeit nicht aktualisiert wurden oder das Abonnement abläuft. Wenn Sie das Produkt nach Ablauf des Abonnements weiterhin verwenden möchten, müssen Sie Ihre Lizenz erneuern.
	Installation	Das Icon erscheint während der Installation des Produktes und gelegentlich bei Updates. Warten Sie, bis der Installationsvorgang abgeschlossen ist.
	Warnung	Eine Funktion von Personal Security Service ist deaktiviert, oder Ihre Virendefinitionen wurden seit längerem nicht aktualisiert.
	Fehler	Ein Fehler ist aufgetreten. Lesen Sie die Fehlermeldung sorgfältig durch.
	Deaktiviert	Das Produkt wurde komplett deaktiviert und ist somit nicht funktionsfähig.
	Fortschrittsanzeige	Der Fortschrittsbalken zeigt an, wie weit der Download von aktuellen Virendefinitionen und Softwareupdates fortgeschritten ist. Bei einer Installation erscheint in der Regel ein Fenster mit Fortschrittsbalken.
	Kein Symbol	Das Programm ist nicht installiert oder es konnte wegen eines Fehlers nicht geladen werden. Ihr Computer ist nicht geschützt. Starten Sie den Computer neu. Wenn auch weiterhin kein Symbol angezeigt wird, installieren Sie das Programm neu.

1. Personal Security Service installieren

1.1 Vor der Installation

Systemanforderungen

Ihr Computer muss den folgenden Anforderungen entsprechen, damit Personal Security Service installiert und ausgeführt werden kann:

Prozessor	Intel Pentium® II 300 MHz oder höher
Betriebssystem	Microsoft® Windows® 98/ME/2000/XP
Arbeitsspeicher (minimal)	Windows 98/ME: 64 MB RAM Windows 2000/XP: 128 MB RAM
Arbeitsspeicher für AntiVirus, Internet-Schutzschild, Anti Spam und SurfControl	Windows 98/ME: 128 MB RAM Windows 2000/XP: 256 MB RAM
Festplattenspeicher (minimal)	130 MB freier Festplattenspeicherplatz (200 MB bei der Installation)
Festplattenspeicher für AntiVirus, Internet-Schutzschild, Anti Spam und SurfControl	210 MB freier Festplattenspeicherplatz (300 MB bei der Installation)
Bildschirm	Mindestens 256 Farben
Internetverbindung	Eine Internetverbindung ist zur Validierung Ihrer Anmeldung und zum Empfangen von Aktualisierungen erforderlich
Browser	Internet Explorer 3.0 oder höher

Den Computer für die Installation vorbereiten

Das gleichzeitige Ausführen verschiedener Anti-Virus- und Firewall-Programme ist nicht möglich. Durch Konflikte zwischen Anti-Virus-Softwares können Ihre Dateien unter Umständen beschädigt werden oder es kann zu einem Systemausfall kommen.

Andere Anti-Virus- bzw. Firewall-Software entfernen

Anti-Virus- und Firewall-Programme von anderen Herstellern müssen einzeln deinstalliert werden, bevor Personal Security Service installiert werden kann. Anweisungen zum Deinstallieren der Software finden Sie in den entsprechenden Dokumentationen dieser Hersteller.

Weiterführende Hinweise:

- Die Nutzung eines Registrierungsschlüssels ist jeweils nur auf einem PC möglich; er ist immer auf dem PC aktiv, auf dem er zuletzt freigeschaltet wurde.
- Sofern Sie zwei oder mehrere Schlüssel besitzen und Sie einen oder mehrere Schlüssel wieder auf einem PC installieren möchten, auf dem der Schlüssel bereits genutzt wurde und ein weiterer Registrierungsschlüssel aktiv war, ist es notwendig, die bisherige Installation rückgängig zu machen. Personal Security Service muss in diesem Fall deinstalliert werden, um den Registrierungsschlüssel verwenden zu können.

1.2 Installation von der Personal Security Service CD

Hinweis: Wenn Sie Windows 2000 oder Windows XP verwenden und über mehr als ein Benutzerkonto verfügen, müssen Sie sich als Administrator anmelden, um Personal Security Service zu installieren.

Wie kommen Sie an den Registrierungsschlüssel zur Freischaltung der Software?

- Sofern Sie PSS unter http://www.t-com.de/pss bestellt haben, wird Ihnen der Registrierungsschlüssel per E-Mail zugesandt. Dies dauert ca. zwei Werktage.
- Wenn Sie noch nicht über einen Registrierungsschlüssel verfügen, finden Sie entweder im Internet unter http://www.t-com.de/pss einen Button zum Bestellen vor oder Sie kaufen z. B. im T-Punkt die T-TeleSec Personal Security Service CD als Software-Paket für ein Jahr.
- Wenn Sie die T-TeleSec Personal Security Service CD im Handel erworben haben, dann entnehmen Sie den Registrierungsschlüssel der Rückseite des Handbuches.

Führen Sie zur Installation von Personal Security Service über CD die folgenden Schritte aus:

1. Schließen Sie alle anderen Programme, und legen Sie die Personal Security Service CD in das CD-ROM-Laufwerk Ihres Computers ein.
2. Sollte sich das Startmenü nicht automatisch öffnen, dann wählen Sie das CD-ROM-Laufwerk und klicken Sie auf die Datei autorun.exe. Danach öffnet sich das Startmenü.
3. Klicken Sie auf setup.exe. Die Installation wird gestartet.
4. Wählen Sie die Sprache, in der die Installation ausgeführt werden soll, und klicken Sie auf **Weiter.**
5. Lesen Sie die angezeigten Hinweise zur Installation von Personal Security Service sorgfältig durch. Zum Fortfahren der Installation klicken Sie auf **Weiter.**
6. Lesen Sie die Lizenzbedingungen des Software-Herstellers durch, und aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Vereinbarung** per Mausklick, wenn Sie den Bedingungen zustimmen. Klicken Sie auf **Weiter,** um fortzufahren.
7. Wählen Sie das Verzeichnis, in dem Personal Security Service installiert werden soll. Klicken Sie auf **Weiter,** um fortzufahren.
8. Es werden Dateien auf Ihren Computer übertragen. Wenn die Übertragung abgeschlossen ist, werden Sie zur Eingabe des Registrierungsschlüssels (Anmeldenummer) aufgefordert.
9. Geben Sie Ihren Registrierungsschlüssel nach Aufforderung durch die Software ein. Sofern Sie online bestellt haben, kopieren Sie dazu am besten den Registrierungsschlüssel aus der E-Mail und fügen Sie diesen dann in das erste Feld ein und klicken Sie auf **Weiter.** Nachdem Ihr Registrierungsschlüssel erfolgreich geprüft wurde, startet die Installation der Personal Security Service Software.
   Beachten Sie, dass zur Prüfung der Gültigkeit des Registrierungsschlüssels eine aktive Internetverbindung erforderlich ist.

Tipp: Sie können den Fortschritt des Installationsprozesses verfolgen, indem Sie sich in der Windows-Systemleiste rechts unten auf dem Bildschirm das Icon ansehen. Das folgende Symbol erscheint, sobald die Installation abgeschlossen ist:

Hinweis: Nach erfolgreich durchgeführter Installation erscheint der Startup-Assistent von Personal Security Service. Siehe Kapitel 1.5 Startup-Assistent auf Seite 14.

10. Nachdem Personal Security Service die erforderlichen Dateien installiert hat, werden Sie aufgefordert, den Computer neu zu starten. Wählen Sie **Jetzt neu starten** (wenn Sie **Später neu starten** wählen, wird die Installation erst abgeschlossen, wenn der Computer neu gestartet wurde). Klicken Sie auf **OK,** um die Installation abzuschließen.
    Unter 2.4 Erstmaliges Verwenden des Programms auf Seite 21 erfahren Sie, wie sich feststellen lässt, ob die Installation erfolgreich war.

Hinweis: Nach Abschluss der Installation zeigen Ihnen sowohl die Anwendungssteuerung als auch die Dialerschutz-Funktion in einer Meldung an, dass Sie festlegen müssen, welche Anwendungen bzw. Wählverbindungen zum Internet herstellen dürfen und welche nicht. Weitere Informationen hierzu finden Sie unter 2.2 Vorgehensweise bei Anzeige des Anwendungssteuerungs-Pop-ups auf Seite 18 und unter Dialerschutz im Kapitel 5.7 auf Seite 78.

1.3 Installation von Personal Security Service über das Internet

Hinweis: Wenn Sie Windows 2000 oder Windows XP verwenden und über mehr als ein Benutzerkonto verfügen, müssen Sie sich als Administrator anmelden, um Personal Security Service zu installieren.

Führen Sie zur Installation von Personal Security Service über das Internet die folgenden Schritte aus:

1. Wenn Sie noch nicht über einen Registrierungsschlüssel verfügen, finden Sie unter http://www.t-com.de/pss einen Button zum Bestellen vor. Der Registrierungsschlüssel wird Ihnen dann per E-Mail zugesandt. Dies dauert ca. zwei Werktage.
2. Wenn Sie bereits über einen Registrierungsschlüssel verfügen, können Sie direkt fortfahren.
3. Laden Sie sich unter https://pss.t-com.de/download/installer.exe das Installationsprogramm installer.exe herunter.
4. Nachdem Sie installer.exe (ca. 9 MB) heruntergeladen haben, öffnen Sie den Ordner Arbeitsplatz auf Ihrem Rechner und wählen Sie den Ordner aus, in dem Sie installer.exe gespeichert haben.
5. Doppelklicken Sie auf die Datei installer.exe. Die Installation wird gestartet.

6. Wählen Sie die Sprache, in der die Installation ausgeführt werden soll, und klicken Sie auf **Weiter.**
7. Lesen Sie die angezeigten Hinweise zur Installation von Personal Security Service sorgfältig durch. Zum Fortfahren der Installation klicken Sie auf **Weiter.**
8. Lesen Sie die Lizenzbedingungen des Software-Herstellers durch, und aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Vereinbarung** per Mausklick, wenn Sie den Bedingungen zustimmen. Klicken Sie auf **Weiter,** um fortzufahren.
9. Wählen Sie das Verzeichnis, in dem Personal Security Service installiert werden soll. Klicken Sie auf **Weiter,** um fortzufahren.
10. Geben Sie Ihren Registrierungsschlüssel nach Aufforderung durch die Software ein. Kopieren Sie dazu am besten den Registrierungsschlüssel aus der E-Mail, und fügen Sie diesen dann in das erste Feld ein, und klicken Sie auf **Weiter.** Nachdem Ihr Registrierungsschlüssel erfolgreich geprüft wurde, startet die Installation der Personal Security Service Software. **Beachten Sie, dass zur Prüfung der Gültigkeit des Registrierungsschlüssels eine aktive Internetverbindung erforderlich ist.**

Tipp: Sie können den Installationsprozess verfolgen, wenn Sie in der Windows-Systemleiste rechts unten auf dem Bildschirm auf doppelklicken. Das Symbol wird durch ersetzt, sobald die Installation abgeschlossen ist.

Hinweis: Nach erfolgreich durchgeführter Installation erscheint der Startup-Assistent von Personal Security Service. Siehe Kapitel 1.5 Startup-Assistent auf Seite 14.

11. Nachdem Personal Security Service die erforderlichen Dateien installiert hat, werden Sie aufgefordert, den Computer neu zu starten. Wählen Sie **Jetzt neu starten** (wenn Sie **Später neu starten** wählen, wird die Installation erst abgeschlossen, wenn der Computer neu gestartet wurde). Klicken Sie auf **OK,** um die Installation abzuschließen.
    Unter 2.4 Erstmaliges Verwenden des Programms auf Seite 21 erfahren Sie, wie sich feststellen lässt, ob die Installation erfolgreich war.

Achtung: Bei Registrierungsschlüsseln mit SurfControl erscheint nach erfolgreich durchgeführter Installation ein Fenster, in dem das Passwort für SurfControl festgelegt werden muss. Mit Hilfe von SurfControl können Sie unerwünschte Webseiten

blockieren und den Zugriff auf die Programmeinstellungen einschränken. Dieses Passwort muss bei Änderungen an den Produkteinstellungen eingegeben werden.



Hinweis: Nach Abschluss der Installation zeigen Ihnen sowohl die Anwendungssteuerung als auch die Dialerschutz-Funktion in einer Meldung an, dass Sie festlegen müssen, welche Anwendungen bzw. Wählverbindungen zum Internet herstellen dürfen und welche nicht. Weitere Informationen hierzu finden Sie unter 2.2 Vorgehensweise bei Anzeige des Anwendungssteuerungs-Pop-ups auf Seite 18 und unter Dialerschutz im Kapitel 5.7 auf Seite 78.

1.4 Wenn Personal Security Service deinstalliert werden muss

Hinweis: Wenn Sie Windows NT 4.0, Windows 2000 oder Windows XP verwenden und über mehr als ein Benutzerkonto verfügen, müssen Sie sich als Administrator anmelden, um Personal Security Service zu deinstallieren.

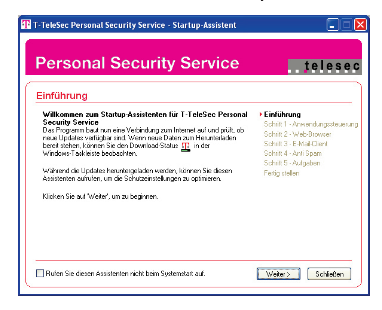
Deinstallieren Sie Personal Security Service mit Hilfe des Windows-Startmenüs. Hierdurch wird das Programm von Ihrem Computer entfernt. Gehen Sie dazu folgendermaßen vor:

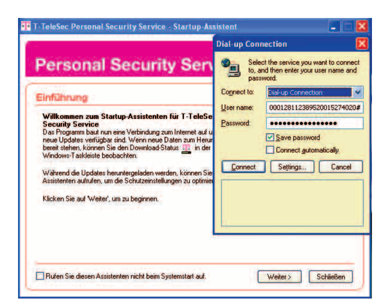
1. Öffnen Sie in der Windows-Taskleiste das Startmenü.
2. Wählen Sie Programme → Personal Security Service → Personal Security Service deinstallieren.
3. Das Programm fordert Sie auf, den Deinstallationsvorgang zu bestätigen:
   a. Klicken Sie auf **Nein,** wenn Sie die Software nicht deinstallieren möchten.
   b. Klicken Sie auf **Ja,** wenn Sie die Software löschen möchten, und führen Sie die nachfolgenden Schritte aus.

4. Warten Sie einen Moment. Der Deinstallationsvorgang kann einige Minuten dauern. Wenn dieser abgeschlossen ist, klicken Sie auf **Fertig.**
5. Starten Sie den Computer nach der Deinstallation neu.
6. Ein Ordner mit dem Namen Personal Security Service, der sich jetzt ggf. noch auf der Festplatte befindet, kann von Ihnen gelöscht werden. Personal Security Service ist danach von Ihrem Computer gelöscht.

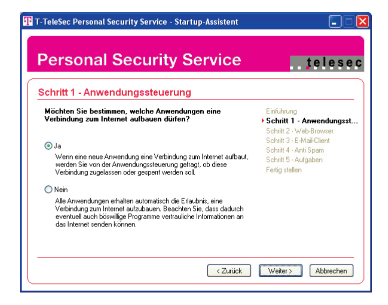
1.5 Startup-Assistent

Nach erfolgreich durchgeführter Installation erscheint der Startup-Assistent von Personal Security Service. Der Startup-Assistent sorgt zum einen dafür, dass vor der erstmaligen Aktivierung des Produktes alle aktuellen Virendefinitionen sowie Updates verfügbar sind und Sie so auf dem aktuellsten Stand hinsichtlich der Sicherheit sind. Zum anderen können Sie im Startup-Assistenten festlegen, welche Standardprogramme Sie verwenden. Die Software erkennt dann, dass diese Anwendung vertrauenswürdig ist und fragt Sie bei der Benutzung der Software nicht mehr explizit, ob Sie die Applikationen zulassen möchten. Ihr System wird durch diese Einstellungen optimiert.





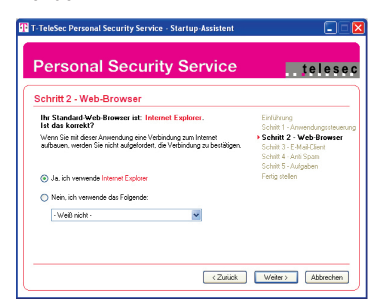
Das Programm fordert Sie auf, eine Internetverbindung aufzubauen, damit es überprüfen kann, ob neue Updates zum Download bereitstehen. Wenn ja, lädt Personal Security Service diese automatisch herunter. Während des Downloads können Sie Ihre Standardprogramme festlegen, indem Sie auf **Weiter** klicken.



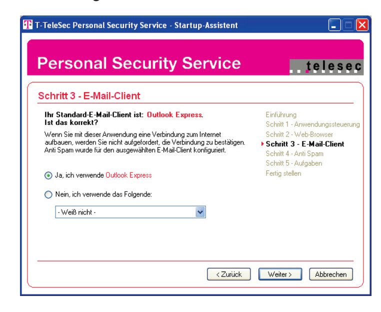
Hier können Sie festlegen, ob Sie bei jeder Applikation einzeln die Entscheidung über die Zulassung fällen möchten, ob diese zugelassen werden darf oder nicht. Bei bereits bekannten zugelassenen oder abgelehnten Applikationen erscheint kein Entscheidungsfenster. Aber nur dann, wenn man die Einstellung vorgenommen hat, dass sich die Software die Einstellung merken soll.

Sie können hier auch festlegen, dass alle Applikationen zugelassen werden sollen, ohne Sie danach zu fragen. Diese Einstellung/Konfiguration ist jedoch nicht empfehlenswert, weil bösartige Programme diese Einstellung zu ihren Zwecken ausnutzen könnten.

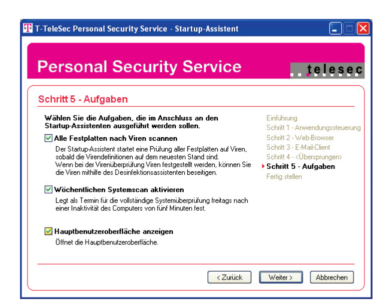
Bitte legen Sie bei den folgenden Fenstern fest, welche Standardprogramme Sie verwenden:



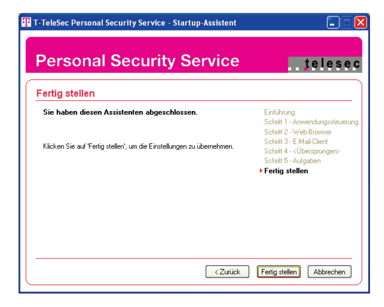
Hier legen Sie fest, mit welchem Browser, z.B. Internet Explorer, Mozilla etc., Sie ins Internet gehen.



Hier legen Sie Ihr Standard-E-Mail-Programm fest.



Hier können Sie nun auswählen, ob der Virenscanner direkt im Anschluss alle Ihre Festplatten auf Viren überprüfen soll, ob Sie einen Zeitplan für regelmäßige Virenüberprüfungen festlegen möchten und ob sich direkt im Anschluss die grafische Benutzeroberfläche öffnen soll.



Nachdem alle Einstellungen getätigt wurden, können Sie den Vorgang mit der Bestätigung des Buttons **Fertig stellen** abschließen.

Hinweis: Falls Sie sich für den anschließenden Virenscan entscheiden, bedenken Sie, dass der Scan-Vorgang je nach Speicherplatz Ihres PCs und Anzahl der Dateien auf dem PC einige Zeit in Anspruch nehmen kann.

2. Erste Schritte

2.1 Personal Security Service erstmals verwenden

Wenn Sie Personal Security Service erstmals verwenden, lesen Sie sich die folgenden Abschnitte aufmerksam durch, um zu überprüfen, ob Personal Security Service einwandfrei ausgeführt wird und Ihren Sicherheitsanforderungen gerecht wird.

2.2 Vorgehensweise bei Anzeige des Anwendungssteuerungs-Pop-ups

Bei der Anwendungssteuerung handelt es sich um ein Dienstprogramm, das alle Verbindungen zu oder von der Software zum Internet oder einem beliebigen lokalen Netzwerk überwacht. Abhängig von ihren Einstellungen können Sie entweder alle Verbindungen zulassen und ein Protokoll der einzelnen Verbindungen erstellen lassen oder bei jedem Verbindungsversuch wird ein Fenster mit der Frage angezeigt, ob die Verbindung zugelassen werden soll. Außerdem wird überprüft, ob die Software, die einen Verbindungsaufbau versucht, mit der ursprünglich zugelassenen Software übereinstimmt. Wenn die Software nicht mit der ursprünglich zugelassenen Anwendung übereinstimmt, zeigt die Anwendungssteuerung eine entsprechende Warnung an und fragt den Benutzer, ob das geänderte Programm eine Verbindung aufbauen darf oder nicht.

Beispiel: den Internet-Browser nach der Installation erstmals starten

1. Starten Sie Ihren Internet-Browser (z. B. Internet Explorer, Netscape).



2. Das Anwendungssteuerungs-Pop-up wird angezeigt, in dem Sie angeben müssen, ob der Verbindungsversuch vom Internet Explorer zugelassen oder verhindert werden soll.
   a. Wählen Sie **Diese Einstellung für die Zukunft speichern,** da Ihr Internet-Browser eine sichere Anwendung ist.
   b. Klicken Sie auf die Option zum Zulassen, da der von Ihnen selbst gestartete Browser sicher ist (weitere Informationen dazu, was als sicher bzw. nicht sicher gilt, finden Sie unter 5.5 Anwendungssteuerung auf Seite 68).

Wenn Sie auf **Hilfe** klicken, werden weitere Informationen zur Anwendungssteuerung angezeigt.

Hinweis: Wenn Sie die Anwendungssteuerungs-Funktion deaktivieren möchten, wählen Sie **Internet-Schutzschild** aus. Klicken Sie neben der Anwendungssteuerung auf **Ändern.** Der Statustext wird von **Anzeigen einer Eingabeaufforderung** zu **Zulassen und protokollieren** geändert.

Weitere Informationen zur Anwendungssteuerung finden Sie unter 5.5 Anwendungssteuerung auf Seite 68.

2.3 Vorgehensweise bei Anzeige des Fensters vom Dialerschutz

Wenn Sie den Dialerschutz installiert haben und versuchen, eine DFÜ-Verbindung zum ersten Mal zu öffnen, wird ein entsprechendes Bestätigungsfenster angezeigt. Mit Hilfe des Dialerschutzes können Sie die Rufnummer überprüfen, bevor eine DFÜ-Verbindung aufgebaut wird. Auf diese Weise können böswillige Dialer (wie z. B. 0190er-Nummern) ohne Ihr Wissen keine DFÜ-Verbindung aufbauen.

Beispiel: erste Anwahl der Einwahlnummer des Internetanbieters (z. B. T-Online) nach der Installation

1. Das Pop-up-Fenster des Dialerschutzes wird mit der Frage eingeblendet, ob die Anwendung eine DFÜ-Verbindung zur im Fenster angezeigten Nummer aufbauen darf.



2. Überprüfen Sie die Nummer sorgfältig, um sicherzustellen, dass die angezeigte Nummer korrekt ist. Wählen Sie anschließend **Diese Einstellung für die Zukunft speichern** und klicken Sie auf **Zulassen.** Die Verbindung wird zugelassen, und die Nummer wird zur Liste der zugelassenen Nummern hinzugefügt.

Hinweis: Falls Sie die Dialerschutz-Funktion deaktivieren wollen, gehen Sie bitte auf die Startseite von Personal Security Service und klicken Sie mit der linken Maustaste auf **Deaktivieren.** Sobald Sie den Dialerschutz erfolgreich deaktiviert haben, erscheint ein blauer Kreis mit einem weißen „i“ (für Info) in der Mitte des Kreises.

Weiter gehende Informationen zu der Dialerschutz-Funktion finden Sie unter 5.7 Dialerschutz auf Seite 78.

2.4 Erstmaliges Verwenden des Programms

Wenn Sie das Programm zum ersten Mal verwenden, lesen Sie die folgenden Abschnitte aufmerksam durch, um festzustellen, ob das Programm einwandfrei ausgeführt wird und Ihre Sicherheitsanforderungen erfüllt.

Ist das Programm aktiv, und wird es einwandfrei ausgeführt?

Im Anschluss an die Installation können Sie prüfen, ob das Programm aktiv ist und einwandfrei arbeitet. Klicken Sie dazu auf das Symbol in der Windows-Taskleiste in der rechten unteren Bildschirmecke neben der Uhranzeige.



Hinweis: Unter Windows XP können Symbole ausgeblendet werden. Um ausgeblendete Symbole anzuzeigen, klicken Sie auf die Schaltfläche .

Status-Tooltipp: Platzieren Sie Ihren Mauszeiger über dem Symbol , um die Informationen zum Status anzuzeigen. Anhand dieser Informationen können Sie sofort erkennen, ob beim Programm eine Fehlfunktion vorliegt (wie im nachfolgenden Beispiel, in dem der Virenschutz deaktiviert wurde).



Abhängig vom aktuellen Status wird das Symbol unter Umständen anders oder gar nicht angezeigt. In der nachfolgenden Tabelle finden Sie eine Liste der Symbole mit ihren Bedeutungen:

Symbol	Status	Vorgehensweise
	Das Programm arbeitet einwandfrei. Ihr Computer ist geschützt.	Verwenden Sie Ihre E-Mail-Anwendung und Ihren Internet-Browser wie gewohnt.
	Installation wird ausgeführt. Ihr Computer ist noch nicht geschützt.	Warten Sie, bis der Installationsvorgang abgeschlossen ist. Das Symbol wird im Anschluss an die Installation angezeigt.
	Download wird ausgeführt.	Der Verlauf des Datendownloads wird bei allen Download-Ereignissen angezeigt, wie z. B. Updates der Virendefinitions-Datenbank, von Software oder Sicherheitsprofilen.
	Fehlerstatus. Ein Fehler ist aufgetreten.	Platzieren Sie Ihren Mauszeiger über dem Symbol , um die Ursache für den Fehler anzuzeigen. Starten Sie den Computer gegebenenfalls neu.
	Warnung: Eine Schutzfunktion wurde deaktiviert, oder Ihre Virendefinitionen sind nicht mehr aktuell. Ihr Computer ist nicht vollständig geschützt.	Platzieren Sie Ihren Mauszeiger über dem Symbol , um die Informationen zum Status anzuzeigen. Aktivieren Sie die gegenwärtig deaktivierte Funktion oder überprüfen Sie, ob Updates verfügbar sind. Dieses Warnsymbol wird eventuell bei Systemfunktionen, wie z. B. der Defragmentierung der Festplatte, angezeigt, da einige Systemfunktionen standardmäßig alle Downloads vorübergehend anhalten.
	Kritischer Alarmstatus (blinkendes Symbol).	Dieses Symbol wird angezeigt, wenn die Virendefinitionen in der letzten Zeit nicht aktualisiert wurden oder das Abonnement abläuft. Wenn Sie das Produkt nach Ablauf des Abonnements weiterhin verwenden möchten, müssen Sie Ihre Lizenz erneuern. Sie können über diesen Link auch direkt eine neue Lizenz bestellen: www.t-com.de/pss-bestellung

Symbol	Status	Vorgehensweise
	Nicht geladen. Das Programm ist deaktiviert und Ihr Computer nicht geschützt.	Klicken Sie mit der rechten Maustaste auf das Symbol , und wählen Sie **Erneut laden,** um das Programm zu aktivieren.
Kein Symbol	Das Programm ist nicht installiert oder es konnte wegen eines Fehlers nicht geladen werden. Ihr Computer ist nicht geschützt.	Starten Sie den Computer neu. Wenn auch weiterhin kein Symbol angezeigt wird, installieren Sie das Programm neu.

2.5 Optionen zum Öffnen des Hauptmenüs

Es gibt mehrere Möglichkeiten, um das Programm zu öffnen und es zu verwenden:

Windows-Startmenü

Führen Sie die folgenden Schritte aus, um häufig benötigte Vorgänge auszuführen, die Dokumentation anzuzeigen oder Webseiten aufzurufen:

1. Klicken Sie auf die Windows-Menüschaltfläche **Start.**
2. Öffnen Sie den Ordner **Programme** und den Unterordner **T-TeleSec Personal Security Service.**
3. Klicken Sie auf **T-TeleSec Personal Security Service öffnen,** um das Hauptmenü zu öffnen, oder wählen Sie eine andere Option aus dem Unterordner.

Symbol in der Taskleiste

Über das Symbol in der Windows-Taskleiste (in der unteren rechten Bildschirmecke) können Sie den aktuellen Status anzeigen oder auf das Kontextmenü mit der rechten Maustaste zugreifen. Wenn Sie das Hauptmenü öffnen möchten, doppelklicken Sie auf das Symbol .

Kontextmenü

Klicken Sie mit der rechten Maustaste auf das Symbol , um das Kontextmenü mit einer Liste der gängigsten Operationen zu öffnen. Über dieses Menü können Sie das Hauptmenü öffnen oder sofort nach Viren suchen. In der folgenden Tabelle wird die Bedeutung der einzelnen Menüelemente erläutert:

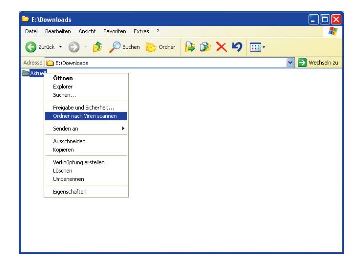
Option	Beschreibung
Öffnen	Öffnet das Hauptmenü. Sie können dort den Status aller Komponenten überprüfen und auf die erweiterten Einstellungen zugreifen, um z. B. Ihre Schutzstufe oder Einstellungen des Spam-Filters zu ändern.
Entladen und mit der aktuellen Sicherheitsstufe fortfahren	Alle Module des Produktes werden deaktiviert außer der Firewall. Die Firewall bleibt weiterhin aktiv mit dem zuletzt von Ihnen ausgewählten Profil.
Entladen und Netzwerkverkehr zulassen	Alle Module des Produktes werden deaktiviert außer der Firewall-Engine. Die Firewall-Engine bleibt weiterhin aktiv wie bei **Entladen und mit der aktuellen Sicherheitsstufe fortfahren,** nur mit dem Unterschied, dass der gesamte Netzwerkverkehr zugelassen ist. Diese Einstellung ist gleichbedeutend mit dem Firewall-Profil **Alle umgehen.**
Virenschutz	
Alle Festplatten scannen	Der Virenschutz scannt alle Festplatten auf Ihrem Computer.
Diskette scannen	Der Virenschutz scannt die Diskette im Laufwerk A.
Ziel scannen ...	Der Virenschutz scannt das von Ihnen angegebene Ziel. Ein Verzeichnisbaum wird angezeigt. Wählen Sie das Zielverzeichnis aus, und klicken Sie auf **OK,** um den Scan-Vorgang zu starten.
Internet-Schutzschild	
Gesamten Datenverkehr blockieren	Der gesamte Netzwerkdatenverkehr wird blockiert. Diese extreme Maßnahme sollte nur angewandt werden, wenn Sie den Verdacht hegen, dass Ihr Computer durch einen Netzwerkangriff bedroht wird oder Sie bereits einen Wurm oder Trojaner auf Ihrem Computer vermuten.
Gesamten Datenverkehr zulassen	Lässt den gesamten Netzwerkdatenverkehr zu. Durch diese Einstellung wird Ihre Firewall deaktiviert, und Ihr Computer ist allen Netzwerkangriffen schutzlos ausgesetzt.
Alarmprotokoll anzeigen	Öffnet das Dialogfeld **Internet-Schutzschild Firewall-Alarme.**

Option	Beschreibung
Anti Spam	
Absender zulassen	Fügt die Adresse des E-Mail-Absenders zur Liste der zugelassenen Absender hinzu. Die Liste der zugelassenen Absender enthält Adressen, die nicht gefiltert und in den Spam-Ordner verschoben werden.
Absender filtern	Fügt die Adresse des E-Mail-Absenders zur Liste der gefilterten Absender hinzu. Die Liste der gefilterten Absender enthält Adressen, die gefiltert und in den Spam-Ordner verschoben werden.
Anti Spam konfigurieren	Öffnet die Anti-Spam-Einstellungen.
SurfControl	
Webseitenfilter aussetzen	Setzt den Webseitenfilter aus. Solange der Webseitenfilter angehalten ist, werden Webseiten nicht blockiert oder protokolliert.
Webseiten-Liste anzeigen	Zeigt die Webseiten-Liste für SurfControl an. Hier können Sie den Zugriff auf zugelassene und gesperrte Webseiten konfigurieren.
Info ...	Zeigt Informationen zum Programm an.

Das Kontextmenü in Windows Explorer und Arbeitsplatz

In Windows Explorer und Arbeitsplatz können Sie Laufwerke, Ordner und Dateien auf Viren scannen. Gehen Sie dazu folgendermaßen vor:

1. Platzieren Sie Ihren Mauszeiger auf dem zu scannenden Laufwerk oder Ordner bzw. der zu scannenden Datei, und klicken Sie mit der rechten Maustaste.
2. Wählen Sie im Kontextmenü **Ordner nach Viren scannen** (die Auswahl hängt vom ausgewählten Objekt ab). Das Fenster **Manuelles Scannen** wird angezeigt, und der Scan-Vorgang wird gestartet.



Bei Feststellung eines Virus wird ein Assistent aufgerufen, der Sie durch die einzelnen Schritte der Desinfektion führt.

2.6 Anlegen eines Spam-Ordners in Ihrer E-Mail-Software

Anti Spam überwacht eingehende E-Mails und entfernt unaufgefordert zugesandte Massen-E-Mails aus Ihrem Posteingang. Anti Spam kann einen Spam-Ordner und die Spam-Filterregeln automatisch in Microsoft Outlook anlegen. Wenn Sie einen anderen E-Mail-Client verwenden, müssen Sie den Spam-Ordner und die Filterregeln manuell anlegen, um Anti Spam zu verwenden. Dieser Abschnitt enthält Anweisungen zum Erstellen des Spam-Ordners und der Filterregeln bei Verwendung von Netscape, Mozilla oder Eudora. Diese Anweisungen eignen sich auch zum Erstellen ähnlicher Filterregeln in anderen E-Mail-Clients, die das Erstellen von Regeln zulassen.

Hinweise: Wenn Sie mehrere E-Mail-Konten benutzen, müssen Sie die Spam-Filterregel für jedes E-Mail-Konto gesondert erstellen. Die Spam-Filterung unterstützt das E-Mail-Protokoll IMAP nicht.

Microsoft Outlook

Benutzer von Microsoft Outlook müssen keinen Spam-Ordner oder Spam-Filterregeln erstellen, da diese automatisch von Anti Spam angelegt werden.

Microsoft Outlook Express

Wenn Sie mit Microsoft Outlook Express arbeiten, erstellt Anti Spam den Spam-Ordner nicht automatisch. Es wird jedoch eine Spam-Filterregel erstellt, die Sie bearbeiten können. Anti Spam fügt die Zeichenfolge [SPAM] am Anfang der Betreffzeile aller Nachrichten ein, die als Spam gefiltert werden. Anti Spam erstellt eine Regel, nach der alle Nachrichten, die die Zeichenfolge [spam] im Betreff enthalten, in den Ordner für gelöschte Objekte verschoben werden. Wenn Sie die Spam-Nachrichten in einen anderen Ordner verschieben möchten, können Sie die Regel manuell bearbeiten. So können Sie die Spam-Nachrichten beispielsweise in einem selbst angelegten Spam-Ordner ablegen, den Sie von Zeit zu Zeit sichten, und ggf. interessante Nachrichten vor dem Leeren des Ordners speichern.

Wichtig: Wird kein eigener Spam-Ordner angelegt und der Ordner für gelöschte Objekte von Outlook automatisch gelöscht, besteht die Gefahr, dass auch für Sie interessante Nachrichten, die als Spam eingestuft wurden, gelöscht werden!

Netscape und Mozilla

So erstellen Sie den Spam-Ordner:

1. Wählen Sie im Menü **Datei** die Option → Neu → Ordner, um ein neues Postfach für Spam-Nachrichten zu erstellen.
2. Geben Sie als Namen für den neuen Ordner Spam ein, und achten Sie darauf, dass der Ordner als Unterordner in Ihrer normalen Profilstruktur erstellt wird.

So erstellen Sie die Spam-Filterregel:

1. Wählen Sie im Menü **Extras** (bei Mozilla „Tools“) die Option → Nachrichten-Filter.
2. Klicken Sie auf **Neu,** um eine neue Filterregel zu erstellen.
3. Geben Sie als Namen der neuen Filterregel Spam ein.
4. Erstellen Sie einen neuen Header-Eintrag, um die Spam-Nachrichten herauszufiltern. Wählen Sie dazu aus der ersten Dropdown-Liste **Anpassen ...**

5. Geben Sie X-Spam-Flag als neuen Nachrichten-Header ein, und klicken Sie auf **Hinzufügen.** Klicken Sie auf **OK,** um das Dialogfeld **Header anpassen** zu schließen.
6. Erstellen Sie eine Regel, damit eine Nachricht in den Spam-Ordner verschoben wird, wenn X-Spam-Flag **Yes** enthält. Dazu wählen Sie aus der ersten Dropdown-Liste X-Spam-Flag, aus der zweiten **enthält** und geben in das Textfeld **Yes** als übereinstimmenden Text ein.
7. Aktivieren Sie das Kontrollkästchen **In Ordner verschieben** aus dem Bereich **Diese Aktionen ausführen.**
8. Wählen Sie den Spam-Ordner aus der Dropdown-Liste **In Ordner verschieben.**
9. Klicken Sie auf **OK,** um die neue Spam-Filterregel zu bestätigen.
10. Schließen Sie das Dialogfeld Nachrichten-Filter.

Eudora

So erstellen Sie den Spam-Ordner:

1. Wählen Sie im Menü **Mailbox** (Postfach) → den Befehl **New ...** (Neu).
2. Geben Sie als Namen des neuen Postfachs Spam ein.

So erstellen Sie die Spam-Filterregel:

1. Wählen Sie im Menü **Tools** (Extras) die Option → **Filters** (Filter).
2. Klicken Sie auf **New** (Neu), um eine neue Filterregel zu erstellen.
3. Aktivieren Sie das Kontrollkästchen **incoming** (Eingehend), um den Filter auf eingehende E-Mails anzuwenden.
4. Geben Sie X-Spam-Flag als Header-Eintrag ein.
5. Geben Sie **Yes** (Ja) in das Feld **contains** (enthält) ein.
6. Wählen Sie **Transfer to** (Übertragen an) aus der Dropdown-Liste **Action** (Aktion).
7. Klicken Sie auf **In** (Eingehend), und wählen Sie das Postfach **Spam.**
8. Schließen Sie das Dialogfeld **Filters** (Filter).

T-Online E-Mail

Der T-Online Client bietet keine Filterfunktion nach Absendern von E-Mails. Da er nicht über eine konfigurierbare Filterfunktion nach Mailinhalten verfügt, kann er vom Anti Spam des Personal Security Service nicht unterstützt werden.

Webmail (z. B. web.de, T-Online Webmail, GMX)

Da es sich bei den Webmail-Diensten nicht um einen E-Mail-Client handelt, der lokal auf Ihrem PC installiert ist, lassen sich auch keine spezifischen Regeln für eingehende Mails einrichten. Somit können Sie bei der Benutzung von Webmail-Diensten die Anti-Spam-Funktion der Software nicht nutzen. Bitte nutzen Sie für die Verwendung von Anti Spam einen E-Mail-Client, der das Erstellen von Regeln zulässt (z. B. Outlook, Outlook Express).

2.7 Start-Einstellungen für SurfControl

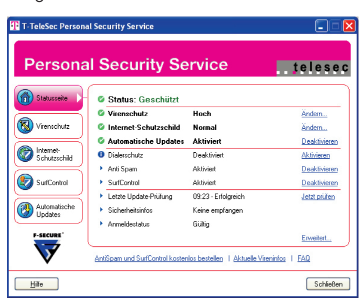
Passwort

Mit Hilfe von SurfControl können Sie unerwünschte Webseiten blockieren und den Zugriff auf die Programmeinstellungen einschränken. Das Passwort für SurfControl wird während der Installation erstellt. Mit diesem Passwort schützen Sie die Programmkonfiguration vor unerwünschten Änderungen.

3. Statusseite



Auf der Statusseite finden Sie eine detaillierte Übersicht über Ihre Sicherheitseinstellungen und den Status aller installierten Komponenten.



Option	Beschreibung
Status	Zeigt den allgemeinen Schutzstatus an. Wenn z. B. länger keine Updates durchgeführt wurden, steht hier der Status **Ungeschützt,** der Ihnen in Rot angezeigt wird.
Virenschutz	Auswahl der Sicherheitsstufe für den Virenschutz.
Internet-Schutzschild	Auswahl der Sicherheitsstufe für den Internet-Schutzschild.
Automatische Updates	Aktivieren und Deaktivieren der automatischen Updates sowie Anzeigen von Informationen zu den auf Ihren Computer heruntergeladenen Updates.
Dialerschutz	Aktivieren und Deaktivieren des Dialerschutzes.
Anti Spam	Aktivieren und Deaktivieren von Anti Spam.
SurfControl	Aktivieren und Deaktivieren von SurfControl.
Letzte Update-Prüfung	Detaillierte Informationen zum letzten Update.
Sicherheitsinfos	Prüfen, ob neue Sicherheitsinfos verfügbar sind.
Anmeldestatus	Detaillierte Informationen zum aktuellen Anmeldestatus.

Option	Beschreibung
Erweitert ...	Öffnet das Fenster **Erweiterte Einstellungen,** um erweiterte Einstellungen zu allen Funktionen vornehmen zu können. Außerdem können Sie über **Erweiterte Einstellungen** Änderungen der Funktionen E-Mail Scanning und Intrusion Prevention vornehmen.

Hinweis: Bitte beachten Sie, dass je nach Registrierungsschlüsseltyp (z. B.: Sie haben nur AntiVirus + Internet-Schutzschild + Anti Spam oder nur AntiVirus + Internet-Schutzschild) nicht alle Komponenten verfügbar sind.

3.1 Anmeldestatus

Auf der Seite **Meine Anmeldung** in den erweiterten Einstellungen können Sie Ihren Anmeldestatus und -typ anzeigen. Zum Öffnen der Seite Meine Anmeldung klicken Sie auf **Erweitert ...** auf der Registerkarte **Start,** öffnen den Zweig **Allgemein** und wählen **Meine Anmeldung.** Klicken Sie auf **Online verlängern,** um einen neuen Registrierungsschlüssel zu erwerben. Sie benötigen eine aktive Internetverbindung. Klicken Sie auf **Schlüssel ändern,** um nach dem Erwerb eines neuen Registrierungsschlüssels diesen einzugeben.

Anmeldestatus

Im Feld **Anmeldestatus** werden Ablaufdatum und -uhrzeit Ihres aktuellen Registrierungsschlüssels angegeben.

- Die Statusangabe **Gültig** bedeutet, dass der Registrierungsschlüssel aktiv ist.
- Die Statusangabe **Abgelaufen** bedeutet, dass der Gültigkeitszeitraum des Registrierungsschlüssels abgelaufen ist.

Anmeldetyp

Der Eintrag **Anmeldetyp** zeigt den Typ Ihres aktuellen Abonnements an.

- Die **Vollständige Lizenz** ist so lange gültig, bis sie gekündigt wird.
- Die **Testlizenz** ist nur zum Testen des Programms gedacht.

Registrierungsschlüssel

Der Eintrag enthält Ihren persönlichen Registrierungsschlüssel zur Nutzung der Software.

3.2 Sicherheitsinfos

Auf den Seiten für die Sicherheitsinfos können Sie sich Berichte zu aktuellen Viren-Bedrohungen und andere Sicherheitsinfos anzeigen lassen. Neben dem Datum und der Uhrzeit der eingegangenen Nachricht wird auch das Thema angezeigt. Die Spalte Schutz enthält Informationen dazu, ob Ihr Computer vor dem betreffenden Virus geschützt ist. Wenn Sie den gesamten Bericht ansehen möchten, doppelklicken Sie auf das Thema, oder markieren Sie den Bericht, und klicken Sie auf **Details ...**
Um alle Sicherheitsinfos aus der Liste zu löschen, klicken Sie auf **Alle löschen.** Wenn beim Empfangen einer Nachricht ein Infofenster eingeblendet werden soll, aktivieren Sie das Kontrollkästchen **Benachrichtigungen auf der Taskleiste signalisieren.**

Detaillierte Beschreibung der Sicherheitsinfos

Im Fenster mit den Eigenschaften der Sicherheitsinfos wird eine Zusammenfassung der ausgewählten Nachricht angezeigt. Am Ende der Zusammenfassung erfahren Sie, ob Ihr Computer bereits vor der Bedrohung geschützt ist. Es gibt vier mögliche Fälle:

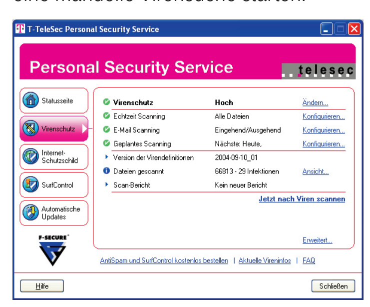
- **Dieser Computer ist noch nicht geschützt. Das Update wird schon bald, bei Erscheinen der Virendefinitionen-Version jjjj-mm-tt_##, verfügbar sein.** Diese Nachricht bedeutet, dass es noch keinen Schutz gegen den Virus gibt. Ein Update, das vor diesem Virus schützt, wird so schnell wie möglich zur Verfügung gestellt.
- **Dieser Computer ist nicht gegen den Virus geschützt. Jetzt aktualisieren ...** Diese Nachricht bedeutet, dass bereits ein Update vorliegt, dieses jedoch noch nicht auf Ihrem Rechner installiert wurde. Klicken Sie auf **Jetzt aktualisieren ...,** um das Programm zu aktualisieren.
- **Dieser Computer ist geschützt.** Ihre Virendefinitionen sind aktuell und schützen Ihren Computer vor dieser Bedrohung.
- **Dieser Computer kann nur mit dem Internet-Schutzschild geschützt werden. Weitere Informationen zum Schutz des Computers finden Sie in der Beschreibung.** Die in dieser Nachricht genannte Malware (schädliches Programm) verursacht Schäden durch Netzwerkangriffe. Die einzige Möglichkeit, Ihren Computer vor derartigen Angriffen zu schützen, besteht in der Konfiguration des Internet-Schutzschildes, um unbefugte Zugriffe auf Ihren Computer zu verhindern.

Klicken Sie auf **Weiter,** um weitere Nachrichten zu lesen. Klicken Sie auf **Schließen,** um das Fenster zu schließen.

4. Virenschutz



Der Virenschutz stoppt Viren (siehe Glossar) und böswilligen Code. Diese Malware greift über E-Mails, das Internet oder Wechseldatenträger automatisch in Echtzeit an. Durch E-Mail Scanning wird überprüft, dass keine Viren via E-Mail versendet oder empfangen werden. Auf der Registerkarte **Virenschutz** finden Sie die wichtigsten Informationen, die Ihren Virenschutzstatus betreffen. Von dieser Registerkarte aus können Sie die wichtigsten Virenschutzeinstellungen wie die gewünschte Stufe für den Echtzeitschutz, Optionen zum Überprüfen von E-Mails sowie geplante Scan-Vorgänge direkt ändern. Darüber hinaus können Sie die Scan-Berichte anzeigen oder eine manuelle Virensuche starten.



Option	Beschreibung
Virenschutz	Folgende Profile stehen zur Auswahl: **Hoch, Normal, Benutzer-definiert** oder **Aus.** Bei deaktiviertem Virenschutz ist der Computer Virenangriffen schutzlos ausgeliefert. Sie können die Virenschutzstufe ändern, indem Sie auf **Ändern ...** klicken.
Echtzeit Scanning	**Alle Dateien, Bekannte Dateitypen** oder **Deaktiviert.** Zeigt an, ob beim Echtzeit Scanning alle Dateien oder alle Dateien der festgelegten Dateitypen überprüft werden oder ob die Funktion deaktiviert wurde. Um die Einstellungen für das Echtzeit Scanning zu ändern, klicken Sie auf **Konfigurieren ...** Jedoch lassen sich die Einstellungen nur abhängig vom Virenschutz-Profil ändern.

Option	Beschreibung
E-Mail Scanning	**Deaktiviert, Eingehend, Ausgehend oder Eingehend/Ausgehend.** Zeigt an, ob die Überprüfung von E-Mails für eingehende und/oder ausgehende E-Mails deaktiviert oder aktiviert ist. Um die Einstellungen für die Überprüfung von E-Mails zu ändern, klicken Sie auf **Konfigurieren ...** Jedoch lassen sich die Einstellungen nur abhängig vom Virenschutz-Profil ändern.
Geplantes Scanning	Hier wird entweder angegeben, dass der Zeitplan für geplante Scan-Vorgänge deaktiviert wurde, oder Datum und Uhrzeit der nächsten geplanten Überprüfung werden angezeigt. Um einen Zeitplan festzulegen, klicken Sie auf **Konfigurieren ...**
Version der Virendefinitionen	Zeigt die Versionsnummer der momentan auf Ihrem Computer verwendeten Software an. Um sicherzugehen, vergleichen Sie die Version der Virendefinitionen mit der Version, die in den Vireninfos angegeben wird.
Dateien gescannt	Zeigt die Anzahl der gescannten Dateien an.
Scan-Bericht	Zeigt den Status der Scan-Berichte an. Wenn es neue Berichte gibt, die Sie noch nicht gelesen haben, wird als Status **Neuer Bericht verfügbar** angezeigt. Wenn Sie den letzten Bericht bereits gelesen haben, wird als Status **Kein neuer Bericht** angezeigt.
Jetzt nach Viren scannen	Beginnt sofort mit der Überprüfung des Systems, um nach Viren zu suchen. Hier können Sie eine der folgenden Optionen auswählen: **Alle lokalen Festplatten scannen, Diskette scannen** oder **Ordner zum Scannen auswählen ...**
Erweitert	Öffnet die Registerkarte Virenschutz im Fenster **Erweiterte Einstellungen.**

4.1 Virenschutz-Profile

Mit Hilfe der Virenschutzstufen können Sie die Schutzstufe jederzeit an Ihre Anforderungen anpassen. Wenn Sie in einer aktuellen Sicherheitsstufe eine beliebige Einstellung ändern (über die erweiterten Einstellungen für den Virenschutz), werden die Änderungen für diese gespeichert. Eine Erläuterung der einzelnen Virenschutzprofile finden Sie in der Software.

Ändern des Virenschutzprofils

Sie können Ihre Virenschutzstufe jederzeit an den erforderlichen Schutz anpassen. Durch das Ändern der ausgewählten Schutzstufe wird die Sicherheitsstufe für automatisierte Vorgänge und Berichtsfunktionen geändert. Gehen Sie folgendermaßen vor, um die Sicherheitsstufe im Abschnitt Virenschutz zu ändern:

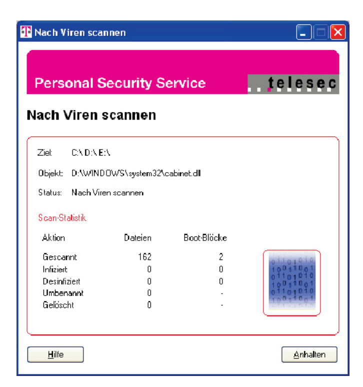
1. Klicken Sie auf **Ändern ...**
2. Wählen Sie aus der Dropdown-Liste eine Schutzstufe aus. Lesen Sie sich die angezeigte Beschreibung der jeweiligen Stufe aufmerksam durch, bevor Sie die Stufe aktivieren.
3. Klicken Sie auf **OK,** um die ausgewählte Schutzstufe zu verwenden.

Hinweis: Bei den Schutzstufen **Hoch** oder **Normal** können Sie einige Virenschutzeinstellungen nicht ändern. Wählen Sie als Virenschutzstufe **Benutzerdefiniert,** wenn Sie alle Einstellungen manuell bearbeiten möchten.

4.2 Nach Viren scannen

Bei aktiviertem Virenschutz ist Ihr Computer geschützt. Beim Öffnen oder Schließen von Dateien werden diese automatisch nach Viren gescannt. Wenn Sie den Verdacht haben, dass eine bestimmte Datei einen Virus enthält, können Sie nur diese Datei oder auch Ihren gesamten Computer manuell nach Viren scannen. Gehen Sie wie folgt vor, um Dateien manuell zu scannen:

1. Klicken Sie auf die Schaltfläche **Jetzt nach Viren scannen.**
2. Wählen Sie im Menü aus, ob alle lokalen Festplatten, eine Diskette oder ein bestimmter Ordner gescannt werden soll.
3. Das Fenster **Manuelle Scan-Statistik** wird angezeigt, in dem die Statistikwerte für den Scan aufgeführt sind. Klicken Sie auf **Anhalten,** um den Scan zu unterbrechen.

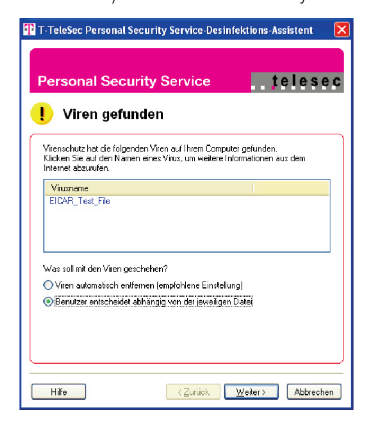


4. Nach Abschluss des Scan-Vorgangs wird ein Bericht erstellt. Klicken Sie auf **Bericht anzeigen,** um den Bericht im Webbrowser anzuzeigen. Wenn ein Virus festgestellt wird:

4.3 Viren vom Computer entfernen

So entfernt der Desinfektions-Assistent von Personal Security Service einen gefundenen Virus. Der Desinfektions-Assistent von Personal Security Service wird angezeigt, wenn

- beim Virusscan ein Virus gefunden wurde,
- ein Virus gefunden wurde und Ihr Virenschutzprofil darauf eingestellt ist, alle Ergebnisse anzuzeigen und Sie vor der Desinfektion zu benachrichtigen,
- bei einem automatischen Scan ein Virus gefunden wurde (automatischer Schutz ist aktiviert) und Personal Security Service den Virus nicht selbst entfernen konnte.



Befolgen Sie zum Entfernen des Virus die folgenden Schritte.

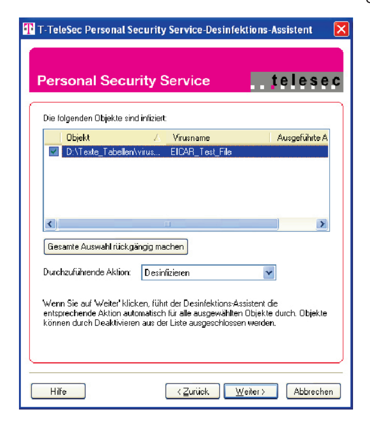
Schritt 1: Virus festgestellt

Der Name des gefundenen Virus wird wie oben angegeben angezeigt. Klicken Sie auf **Weiter,** um mit der Virendesinfektion fortzufahren.

Hinweis: Weitere Informationen zum Virus erhalten Sie, indem Sie auf den Namen des Virus und anschließend auf die Schaltfläche **Vireninfo** klicken. Falls es sich um einen neuen Virus handelt, ist er unter Umständen in der Datenbank noch nicht aufgeführt. Suchen Sie im F-Secure Computerviren-Infocenter unter http://www.f-secure.com/v-descs/ nach den aktuellsten Informationen.

Schritt 2: Durchzuführende Aktion

Eine Liste mit infizierten Dateien wird angezeigt.



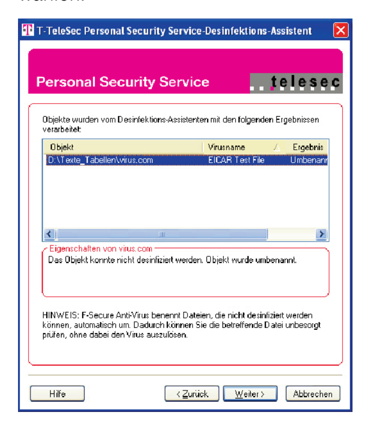
Wählen Sie im Feld **Durchzuführende Aktion** die Aktion aus, die hinsichtlich der infizierten Dateien durchgeführt werden soll. In der nachfolgenden Tabelle finden Sie eine Übersicht über die einzelnen Aktionen.

Aktion	Erklärung
Desinfizieren	Der Desinfektions-Assistent desinfiziert die infizierte Datei. **Hinweis:** Wenn der Desinfektions-Assistent die Datei nicht desinfizieren kann, versucht er, sie automatisch umzubenennen.
Löschen	Der Desinfektions-Assistent löscht die Datei, die den Virus enthält. Alle Daten aus dieser Datei gehen dabei verloren. **Warnung:** Wenn Sie auf **Löschen** klicken, wird auch das infizierte Objekt gelöscht.
Umbenennen	Der Desinfektions-Assistent benennt die Datei um, so dass diese nicht automatisch ausgeführt werden kann. Dadurch wird verhindert, dass der Virus aktiviert wird.

Klicken Sie, nachdem Sie die auszuführende Aktion ausgewählt haben, auf **Weiter.** Dadurch führt der Desinfektions-Assistent die Aktion automatisch für alle ausgewählten Objekte durch.

Schritt 3: Aktionsergebnisse

Das Ergebnis der Aktion wird angezeigt. Wenn die von Ihnen ausgewählte Aktion fehlgeschlagen ist, können Sie Schritt 2 wiederholen und eine andere Aktion auswählen.



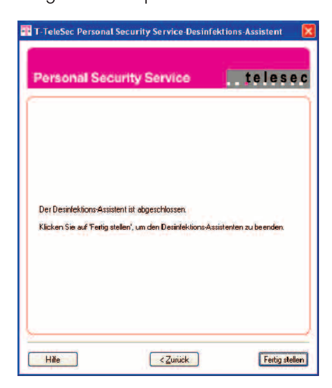
Wenn Desinfektions- oder Löschaktionen fehlschlagen, können Sie die Datei auch umbenennen. Dies ist normalerweise bei infizierten ausführbaren Dateien (.EXE-Dateien) ratsam, da durch die Umbenennung die Erweiterung so geändert wird, dass diese Dateien nicht automatisch ausgeführt werden können. Beachten Sie beim Fehlschlagen von Desinfektions-Aktionen, dass der Desinfektions-Assistent die Datei unter Umständen bereits automatisch umbenannt hat (siehe Aktionstabelle S. 39). Ein Hinweis darauf wird im Feld Eigenschaften angezeigt.

Hinweis: Wenn ein neuer Virus gefunden wurde, die Virendefinitionen veraltet sind oder ein falscher Alarm ausgegeben wird, kann die Desinfektion oder das Löschen fehlschlagen. Anleitungen dazu, was in einem solchen Fall zu tun ist, finden Sie unter Viren nach Fehlschlagen des Desinfektions-Assistenten entfernen auf Seite 41.

Wenn die Aktion erfolgreich war, klicken Sie auf **Weiter,** um fortzufahren.

Schritt 4: Prüfen und Abschließen

Nachdem der Desinfektions-Vorgang abgeschlossen ist, wird ein Desinfektions-Bericht erstellt. Wenn Sie nicht möchten, dass ein Bericht erstellt wird, deaktivieren Sie das Kontrollkästchen **Bericht erstellen.** Beachten Sie, dass der Desinfektionsbericht nicht für Viren erstellt wird, die während eines automatischen Scans gefunden wurden. Klicken Sie auf **Fertig stellen,** um den Desinfektions-Assistenten zu schließen. Der Desinfektions-Bericht wird in Ihrem Standard-Webbrowser angezeigt und enthält Verknüpfungen zu entsprechenden Virenbeschreibungen in der Virendatenbank von F-Secure.



Hinweis: Wenn der Virus in einer Datei gefunden wurde, die beim Löschversuch des Desinfektions-Assistenten durch einen anderen Vorgang gesperrt war, wird ein Fenster angezeigt, das Sie zum Neustart des Computers auffordert. Wenn dieses Fenster angezeigt wird, speichern Sie alle Dokumente und führen Sie dann die im Fenster angezeigten Anweisungen aus.

Viren nach Fehlschlagen des Desinfektions-Assistenten entfernen

Wenn der Desinfektions-Assistent die Datei nicht desinfizieren bzw. löschen konnte, hat dies unter Umständen eine der folgenden Ursachen:

- **Die Virendefinitions-Datenbank ist veraltet.** Überprüfen Sie, ob Sie über die aktuellsten Definitionsdateien verfügen, und versuchen Sie es erneut (siehe Kapitel 8: Automatische Updates auf Seite 100).
- **Falscher Alarm.** Es wurden umfassende Vorkehrungen getroffen, um sicherzustellen, dass Personal Security Service keine harmlosen Dateien als infiziert anzeigt; auf Grund der Komplexität von Dateien kann dies jedoch unter Umständen vorkommen.
- **Es ist eine manuelle Desinfektion erforderlich.** In einigen Fällen müssen Sie ein Programm ausführen, das die Datei desinfiziert und den Virus entfernt. Dieser Fall tritt häufig bei neueren Viren ein, die sich mit Hilfe raffinierter Techniken verstecken und an Ihre Dateien anhängen.
- **Sie haben einen neuen Virus entdeckt.** Ihr Computer ist unter Umständen durch einen neuen Virus infiziert worden. Kein Grund zur Panik. Ihre Dateien sind geschützt, da Personal Security Service den Virus entdeckt und gestoppt hat, bevor dieser Schaden anrichten konnte.

Wenn Sie sich sicher sind, dass die Datei nicht infiziert ist, können Sie die Warnungen ignorieren. Sie können den automatischen Schutz und das manuelle Scannen konfigurieren, um diese Datei bei zukünftigen Scans zu übergehen. Anweisungen dazu finden Sie im Abschnitt 4.5.1 Echtzeit Scanning auf Seite 44 und im Abschnitt 4.5.4 Manuelles Scanning auf Seite 52.

Manuelles Entfernen von Viren

1. Versuchen Sie, die Datei selbst zu desinfizieren. Weitere Hilfe zum Entfernen des Virus finden Sie auch hier:
   - Über den Link **Aktuelle Vireninfos** im Hauptmenü

   oder
   - Suchen Sie im F-Secure Computerviren-Infocenter unter http://www.f-secure.com/v-descs/ nach Informationen zu den Viren. Die Vireninformationen erleichtern Ihnen das Entfernen des Virus und enthalten unter Umständen Verknüpfungen zu den für das Entfernen erforderlichen Programmen.
   - Erfahrene Benutzer: Geeignete Desinfektions-Programme finden Sie direkt unter ftp://ftp.europe.fsecure.com/anti-virus/tools/

   Die Programme enthalten alle erforderlichen Anweisungen, die Sie zum Entfernen des Virus aus Ihrem System ausführen müssen.
2. Wenn der Desinfektions-Assistent fehlgeschlagen ist, Ihre Virendefinitions-Datenbank auf dem aktuellsten Stand ist und das Ausführen von Desinfektions-Programmen von der F-Secure Webseite erfolglos war, befolgen Sie die Anweisungen unter Vorgehensweise bei Feststellen eines neuen Virus im folgenden Abschnitt.

4.4 Vorgehensweise bei Feststellen eines neuen Virus

Wenn Personal Security Service eine Warnung anzeigt, dass eine Datei mit einem Virus infiziert ist, aber den Virus nicht benennen und nicht desinfizieren oder entfernen kann, handelt es sich unter Umständen um einen neuen Virus. Sie sollten diese Datei erst wieder verwenden, wenn Sie sicher sind, dass der Virus entfernt wurde, bzw. wenn klar ist, dass ein falscher Alarm vorlag. Führen Sie zum Entfernen des Virus die folgenden Schritte aus:

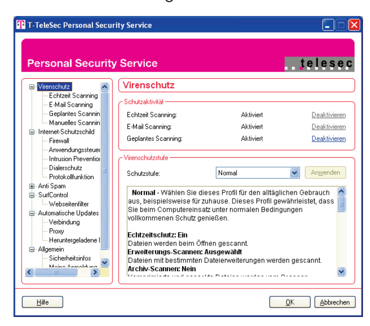
1. Überprüfen Sie, ob Ihre Virendefinitions-Datenbank auf dem aktuellsten Stand ist. Eine aktuellere Definitionsdatei stellt Personal Security Service unter Umständen die Informationen zur Verfügung, die zum Entfernen des Virus von Ihrem Computer benötigt werden.
2. Wenn Sie bereits über die aktuellsten Virendefinitionen verfügen (siehe Kapitel Automatische Aktualisierungen), suchen Sie in den Vireninfos auf der Homepage der Software nach dem Virus. Ggf. wird ein Hinweis darauf gegeben, dass ein

zusätzliches Tool zum Entfernen des Virus notwendig ist. Aktuelle Informationen zu Viren finden Sie auch hier: www.t-com.de/vireninfokatalog

3. Wenn die oben aufgeführten Schritte fehlschlagen, senden Sie die Datei an das F-Secure VirusLab. Anweisungen hierzu finden Sie unter: http://www.f-secure.com/support/technical/general/samples.shtml

4.5 Erweiterter Virenschutz

Auf der Statusseite des Virenschutzes können Sie die zur Verfügung stehenden Funktionen aktivieren und deaktivieren. Um Einstellungen der einzelnen Funktionen vorzunehmen, müssen Sie links im Verzeichnisbaum auf die jeweiligen Komponenten klicken. Die Konfiguration kann nur im Profil **Benutzerdefiniert** erfolgen.

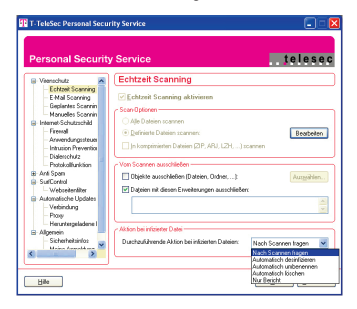


Option	Beschreibung
Echtzeit Scanning	Hier können Sie **Echtzeit Scanning** aktivieren oder deaktivieren, indem Sie mit der rechten Maustaste auf die jeweils unterstrichene Funktion klicken. Die jeweilige Einstellung wird direkt wirksam. Jedoch lassen sich die Einstellungen nur abhängig vom Virenschutz-Profil ändern.
E-Mail Scanning	Hier können Sie **E-Mail Scanning** aktivieren oder deaktivieren, indem Sie mit der rechten Maustaste auf die jeweils unterstrichene Funktion klicken. Die jeweilige Einstellung wird direkt wirksam. Jedoch lassen sich die Einstellungen nur abhängig vom Virenschutz-Profil ändern.

Option	Beschreibung
Geplantes Scanning	Hier können Sie **Geplantes Scanning** aktivieren oder deaktivieren, indem Sie mit der rechten Maustaste auf die jeweils unterstrichene Funktion klicken. Die jeweilige Einstellung wird direkt wirksam. Jedoch lassen sich die Einstellungen nur abhängig vom Virenschutz-Profil ändern.
Virenschutzstufe	Zeigt die zurzeit ausgewählte Schutzstufe an. Wenn Sie die Virenschutzstufe ändern möchten, klicken Sie mit der linken Maustaste auf den Pfeil des Auswahlfeldes. Anschließend werden Ihnen alle zur Auswahl stehenden Schutzstufen angezeigt. Wählen Sie eine neue Stufe aus, indem Sie sich zunächst die Beschreibungen durchlesen und anschließend mit der rechten Maustaste auf den jeweiligen Namen klicken und mit dem Button **Anwenden** die Einstellung bestätigen.

4.5.1 Echtzeit Scanning

Auf der Seite **Echtzeit Scanning** können Sie auswählen, welche Daten in Echtzeit überprüft werden sollen, und bestimmen, wie das Programm weiter vorgehen soll, wenn eine Infektion gefunden wird.



Zum Einschalten des Echtzeit Scanning aktivieren Sie das Kontrollkästchen **Echtzeit Scanning aktivieren.** Wenn Sie den Echtzeitschutz ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Echtzeit Scanning aktivieren.** Mit Hilfe der folgenden Optionen legen Sie fest, was gescannt werden soll:

- **Alle Dateien scannen.** Scannt alle Dateien unabhängig von der Erweiterung. Diese Option ist nicht empfehlenswert, da sie unter Umständen dazu führt, dass das System erheblich langsamer arbeitet.

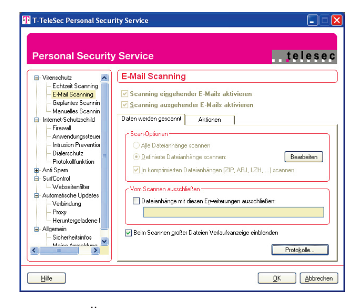
- **Definierte Dateien scannen.** System- und benutzerdefinierte Dateien scannen. Klicken Sie auf **Bearbeiten,** um die gewünschten Dateien zu definieren. Beachten Sie, dass es nicht möglich ist, die vom System festgelegten Dateierweiterungen zu entfernen. Sie können jedoch neue hinzufügen. Geben Sie einen Punkt (.) ein, um Dateien ohne Erweiterung festzulegen. Auch die Verwendung des Fragezeichens (?) als Platzhalter wird unterstützt. Diese Option wird für den Echtzeitschutz empfohlen.
- **In komprimierten Dateien scannen.** Aktivieren Sie dieses Kontrollkästchen, um komprimierte .ZIP-, .ARJ-, .LZH-, .RAR-, .CAB-, .TAR-, .BZ2-, .GZ- und .JAR-Dateien zu scannen. Das Scannen umfangreicher komprimierter Dateien kann unter Umständen viele Systemressourcen in Anspruch nehmen und das System verlangsamen. Dies ist daher für den Echtzeitschutz nicht empfehlenswert.
- **Objekte ausschließen.** Es können einzelne Dateien oder Ordner angegeben werden, die nicht gescannt werden sollen. Klicken Sie dazu auf die Schaltfläche **Auswählen,** um das Dialogfeld **Vom Scannen ausschließen** zu öffnen (siehe Abbildung unten). Wählen Sie in diesem Dialogfeld die Dateien und Ordner aus, die nicht gescannt werden sollen, und klicken Sie auf die Schaltfläche **Hinzufügen.** Um Dateien oder Ordner aus der Liste **Ausgeschlossene Objekte** zu entfernen, wählen Sie die entsprechenden Dateien oder Ordner aus, und klicken Sie auf die Schaltfläche **Entfernen.** Die Dateien oder Ordner werden daraufhin in die Scan-Vorgänge aufgenommen.
- **Dateien mit diesen Erweiterungen ausschließen.** Es können Dateien angegeben werden, die nicht gescannt werden sollen.

Über die Dropdown-Liste **Durchzuführende Aktion** bei infizierten Dateien können Sie festlegen, welche Aktion beim Feststellen einer infizierten Datei durchgeführt werden soll. Wählen Sie eine der folgenden Aktionen aus:

Aktion	Beschreibung
Nach Scannen fragen	Der Desinfektions-Assistent wird gestartet, wenn eine infizierte Datei festgestellt wird.
Automatisch desinfizieren	Die Datei wird automatisch desinfiziert, wenn ein Virus fest-gestellt wird.
Automatisch umbenennen	Die Datei wird automatisch umbenannt, wenn ein Virus gefun-den wird.
Automatisch löschen	Die Datei wird automatisch gelöscht, wenn ein Virus gefunden wird. Diese Option ist nicht empfehlenswert, da dadurch die Datei, an die der Virus angehängt wurde, ebenfalls gelöscht wird.
Nur Bericht	Gibt an, dass ein Virus festgestellt wurde, und verhindert, dass das infizierte Objekt geöffnet wird. Bei Auswahl dieser Option werden Viren nur gemeldet, es wird aber keine Aktion ausge-führt.

4.5.2 E-Mail Scanning

Um die Überprüfung eingehender E-Mails und Anlagen einzuschalten, aktivieren Sie das Kontrollkästchen **Scanning eingehender E-Mails aktivieren.**



Um die Überprüfung ausgehender E-Mails und Anlagen einzuschalten, aktivieren Sie das Kontrollkästchen **Überprüfung ausgehender E-Mails aktivieren.**

4.5.2.1 Scan-Optionen

Mit Hilfe der folgenden Optionen auf der Registerkarte **Scanning** legen Sie fest, was gescannt werden soll:

- **Alle Dateianhänge scannen.** Alle Dateianhänge werden unabhängig von der Dateierweiterung gescannt.
- **Definierte Dateianhänge scannen.** Anlagen mit bestimmten Dateierweiterungen werden gescannt. Klicken Sie auf **Bearbeiten,** um die gewünschten Dateien zu definieren. Geben Sie einen Punkt (.) ein, um Dateien ohne Erweiterung festzulegen. Auch die Verwendung des Fragezeichens (?) als Platzhalter wird unterstützt.
- **In komprimierten Dateianhängen scannen.** Aktivieren Sie dieses Kontrollkästchen, um komprimierte Anlagen vom Typ .ZIP, .ARJ, .LZH, .RAR, .CAB, .TAR, .BZ2, .GZ, .JAR und .TGZ zu scannen. Das Scannen umfangreicher komprimierter Anlagen kann unter Umständen viele Systemressourcen in Anspruch nehmen und das System verlangsamen.
- **Dateianhänge mit diesen Erweiterungen ausschließen.** Sie können auch Dateinamenerweiterungen für Anhänge angeben, die nicht gescannt werden sollen.

Wenn während der Überprüfung großer Dateien bzw. bei vielen Dateien ein Dialogfeld angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Beim Scannen großer Dateien Verlaufsanzeige einblenden.** Klicken Sie auf **Protokolle,** um die TCP/IP-Ports für die Protokolle POP3, IMAP4 und SMTP zu konfigurieren. Standardmäßig verwendet das Programm die Standard-Ports.

4.5.2.2 E-Mail-Aktionen

Auf der Registerkarte **Aktionen** im Dialogfeld **E-Mail Scanning** legen Sie die auszuführenden Aktionen fest, wenn eine infizierte eingehende oder ausgehende E-Mail festgestellt wird. Folgende Aktionen stehen zur Auswahl:

Überprüfung eingehender E-Mails

Aktion bei infizierten Dateianhängen:

- **Desinfizieren –** Wenn ein infizierter Dateianhang gefunden wird, wird der Desinfektions-Assistent gestartet.
- **Entfernen –** Der Anhang wird gelöscht.
- **Keine –** Der Anhang wird ignoriert, aber es wird ein Bericht erstellt.

Aktion bei deformierten Nachrichtenbestandteilen:

- **Entfernen –** Die deformierten Bestandteile der E-Mail werden gelöscht.
- **Keine –** Die deformierten Bestandteile der E-Mail werden ignoriert. Der Vorfall wird jedoch in das Protokoll aufgenommen.

Überprüfung ausgehender E-Mails

Aktion bei infizierten Dateianhängen:

- **Blockieren –** Es wird verhindert, dass die E-Mail gesendet wird.
- **Keine –** Der Anhang wird ignoriert, aber es wird ein Bericht erstellt.

Aktion bei deformierten Nachrichtenbestandteilen:

- **Blockieren –** Es wird verhindert, dass die E-Mail gesendet wird.
- **Keine –** Der Anhang wird ignoriert, aber es wird ein Bericht erstellt.

Aktivieren Sie das Kontrollkästchen **Keine weiteren E-Mails senden, wenn Nachricht blockiert wird,** damit alle weiteren E-Mails blockiert werden. Sie müssen die blockierte E-Mail aus der Warteschlange der ausgehenden E-Mails entfernen, bevor Sie weitere E-Mails senden können. Wenn bei jedem Auffinden einer infizierten E-Mail ein Bericht angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Bericht anzeigen, wenn Infektionen festgestellt wurden.**

4.5.2.3 E-Mail Scanning

Informationen zur Funktionsweise des E-Mail Scannings

E-Mail Scanning überprüft den E-Mail-Verkehr völlig transparent. Eingehende Nachrichten werden gescannt, bevor der E-Mail-Client die E-Mail empfängt, und ausgehende Nachrichten werden nach dem Versand durch den E-Mail-Client, jedoch vor Erreichen des E-Mail-Servers überprüft. Es ist nicht notwendig, die Konfiguration des E-Mail-Clients während der Installation zu ändern.

Beim E-Mail Scanning werden Anhänge und der Nachrichtentext nach schädlichem Code gescannt. Beim Auffinden einer infizierten E-Mail modifiziert das E-Mail Scanning den ursprünglichen Datenstrom, nachdem das Scan-Ergebnis empfangen wurde.

Beispiel: Es ist möglich, einen infizierten Anhang in einer E-Mail standardmäßig zu entfernen oder durch einen desinfizierten Anhang zu ersetzen. Der normale (nicht infizierte) E-Mail-Verkehr wird in keiner Weise beeinträchtigt. Standardmäßig werden Dateiarchive nicht gescannt, eine vollständige rekursive Archivüberprüfung wird

jedoch unterstützt und kann über die Produkteinstellungen aktiviert werden. Alle gesäuberten E-Mails werden mit einer Nachricht versehen. Diese Meldung ist immer englisch und wird nicht übersetzt.

Woran erkenne ich, dass ein Virus in einer E-Mail gefunden wurde?
Sie empfangen eine E-Mail mit dem Hinweis, dass ein Virus in der E-Mail gefunden wurde, diese aber erfolgreich bereinigt werden konnte. Darüber hinaus können Sie sich den Scanning-Bericht anzeigen lassen, um zu sehen, welche Aktionen durchgeführt wurden.

Vor welchen Gefahren schützt E-Mail Scanning?
Das E-Mail Scanning überprüft die gesamte E-Mail-Nachricht. Das E-Mail Scanning scannt nach Viren in verschiedenen Archivformaten, und die Archive sowie binäre Anhänge und eingebettete OLE-Objekte werden rekursiv gescannt.

Warum erhöht sich die Download-Zeit für E-Mails nach der Installation des E-Mail Scannings?
Wenn Sie festlegen, dass das Produkt Archive (z. B. ZIP) in E-Mail-Anlagen scannt, werden die Archive entpackt und alle darin befindlichen Dateien einzeln gescannt. Bei großen Archiven dauert das eine Weile: Die dafür benötigte Zeit entspricht ungefähr der Zeit, die Sie aufwenden müssten, um das Archiv zu entpacken und alle Dateien einzeln mit dem Virenschutz zu scannen. Bei länger andauernden Scans blendet das E-Mail Scanning ein Fenster mit einer Verlaufsanzeige ein, damit Sie die Restdauer ungefähr abschätzen können.

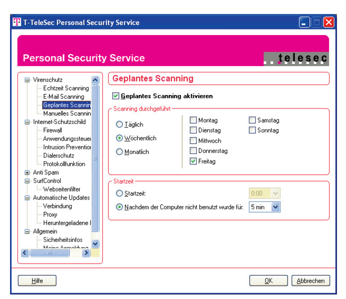
Beschränkungen des E-Mail Scannings
Datenverkehr im SSL-Tunnel wird nicht überprüft, da diese Meldungen erst nach Erreichen des E-Mail-Clients entschlüsselt werden. Ihr Computer ist aber weiterhin geschützt, da alle über SSL empfangenen Anhänge beim Speichern im Cache des lokalen E-Mail-Clients gescannt werden. Außerdem werden vor dem Senden alle Dateien gescannt. Die meisten gängigen Mailbox-Dateiformate des E-Mail-Clients werden standardmäßig gescannt. Die Beschränkung liegt darin, dass E-Mail-Header nicht auf deformierte Bestandteile überprüft werden.

Passwortgeschützte Archive können nicht gescannt werden, da ihr Passwort nicht bekannt ist. Trotzdem besteht kein Grund zur Sorge, da mögliche Viren den Computer erst nach dem Öffnen des Archivs infizieren können. Beim Öffnen des Archivs werden die enthaltenen Dateien gescannt. Solange der Echtzeitschutz aktiviert ist, stellt diese Beschränkung keine Sicherheitsgefahr dar.
E-Mail Scanning arbeitet mit den Standardprotokollen POP und SMTP, die oberhalb von TCP/IP ausgeführt werden. Wenn Ihr E-Mail-Client die elektronische Post mit Hilfe des POP- oder IMAP-Protokolls abruft und zum Versenden das Standardprotokoll SMTP verwendet, wird der E-Mail-Verkehr vom E-Mail Scanning überprüft. Beachten Sie, dass der E-Mail-Scanner keinen Webmail-Datenverkehr wie Hotmail überprüft. E-Mail-Anhänge werden aber in jedem Fall gescannt, wenn sie ausgeführt oder auf der Festplatte gesichert werden.

E-Mail Scanning-Bericht
Wenn das E-Mail Scanning einen infizierten Anhang findet, wird ein Scan-Bericht angezeigt. Im Scan-Bericht können Sie in der Spalte Nachricht feststellen, zu welcher E-Mail der infizierte Anhang gehört. Der Inhalt der Spalte **Grund** gibt Auskunft über die Ursache für den Bericht. Wenn Sie auf den Grund klicken, wird eine Beschreibung des Virus angezeigt. Dazu wird der Browser geöffnet, und die F-Secure Webseiten mit Vireninformationen werden angezeigt. In der Spalte Aktion befinden sich Angaben zu den Maßnahmen, mit denen die E-Mail gesäubert wurde. Wenn dieses Dialogfeld nicht mehr angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Dieses Dialogfeld nicht mehr anzeigen.** Klicken Sie auf **Schließen,** um den Scan-Bericht zu schließen.

Verlaufsdialogfeld beim Scannen von E-Mails
Wenn die Überprüfung der E-Mails viel Zeit in Anspruch nimmt, wird das Verlaufsdialogfeld angezeigt. Sie sehen den Namen des gescannten Anhangs sowie eine Verlaufsleiste, die Ihnen hilft, die verbleibende Dauer abzuschätzen. Große Dateianhänge oder sehr langsame Netzwerkverbindungen sind mögliche Gründe, warum die Überprüfung einer E-Mail länger dauern kann. Wenn dieses Dialogfeld nicht mehr angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Dieses Dialogfeld nicht mehr anzeigen.** Klicken Sie auf **Schließen,** um den Scan-Bericht zu schließen.

4.5.3 Geplantes Scanning

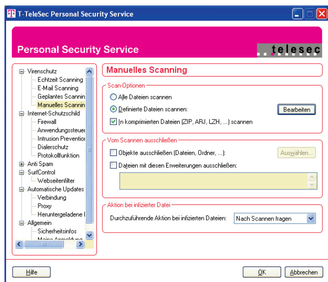


Sie können festlegen, dass der Virenschutz Ihren Computer zu bestimmten Zeiten überprüft. Aktivieren Sie dazu das Kontrollkästchen **Geplantes Scanning aktivieren.** Um einen Zeitplan für die Überprüfung festzulegen, wählen Sie entweder **Täglich, Wöchentlich** oder **Monatlich** unter **Überprüfung durchgeführt.**

- Wählen Sie **Täglich,** wenn der Computer täglich zur geplanten Zeit überprüft werden soll. Die Wochentage auf der rechten Seite sind alle ausgewählt. Sie können diese Auswahl nicht ändern.
- Wählen Sie **Wöchentlich,** um den Computer jede Woche an einem bestimmten Wochentag zur geplanten Zeit zu scannen. Sie können auf der rechten Seite beliebig viele Wochentage auswählen. Die Überprüfung wird dann an jedem dieser ausgewählten Tage durchgeführt.
- Wählen Sie **Monatlich,** um den Computer jeden Monat an einem bestimmten Tag zur geplanten Zeit zu scannen. Sie können bis zu drei Tage des Monats auswählen, an denen die Überprüfung durchgeführt wird. Die Termine sind dabei frei wählbar. (Bei der letzten Option handelt es sich um **Letzter Tag des Monats.** Viele Viren werden am ersten Tag eines Monats aktiviert. Deshalb ist eine Überprüfung des Computers am letzten Tag jeden Monats empfehlenswert.)

Wählen Sie die Startzeit für die Überprüfung aus der Dropdown-Liste **Startzeit** aus. Wenn die Überprüfung nur stattfinden soll, wenn Sie gerade nicht mit dem Computer arbeiten, aktivieren Sie das Kontrollkästchen **Nachdem der Computer nicht benutzt wurde für [x min.],** und wählen Sie die Inaktivitätszeit aus der Dropdown-Liste.

4.5.4 Manuelles Scanning



Mit Hilfe der folgenden Optionen legen Sie fest, was gescannt werden soll:

- **Alle Dateien scannen.** Alle Dateien werden unabhängig von der Dateierweiterung gescannt. Diese Option ist nicht empfehlenswert, da sie unter Umständen dazu führt, dass das System beträchtlich langsamer arbeitet.
- **Definierte Dateien scannen.** Dateien mit bestimmten Dateierweiterungen werden gescannt. Klicken Sie auf **Bearbeiten,** um die gewünschten Dateien zu definieren. Geben Sie einen Punkt (.) ein, um Dateien ohne Erweiterung festzulegen. Auch die Verwendung des Fragezeichens (?) als Platzhalter wird unterstützt. Geben Sie alle Dateierweiterungen ein, und trennen Sie sie durch ein Leerzeichen.
- **In komprimierten Dateien scannen.** Aktivieren Sie dieses Kontrollkästchen, um komprimierte .ZIP-, .ARJ-, .LZH-, .RAR-, .CAB-, .TAR-, .BZ2-, .GZ- und .JAR-Dateien zu scannen. Das Scannen umfangreicher komprimierter Dateien kann unter Umständen viele Systemressourcen in Anspruch nehmen und das System verlangsamen.
- **Objekte ausschließen.** Es können einzelne Dateien oder Ordner angegeben werden, die nicht gescannt werden sollen. Klicken Sie dazu auf die Schaltfläche **Auswählen,** um das Dialogfeld **Vom Scannen ausschließen** zu öffnen (siehe Abbildung unten). Wählen Sie in diesem Dialogfeld die Dateien und Ordner aus, die nicht gescannt werden sollen und klicken Sie auf die Schaltfläche **Hinzufügen.** Um Dateien oder Ordner aus der Liste **Ausgeschlossene Objekte** zu entfernen, wählen Sie die entsprechenden Dateien oder Ordner aus, und klicken Sie auf die Schaltfläche **Entfernen.** Die Dateien oder Ordner werden daraufhin in die Scan-Vorgänge aufgenommen.
- **Dateien mit diesen Erweiterungen ausschließen.** Es können Dateien angegeben werden, die nicht gescannt werden sollen.

Über die Dropdown-Liste **Durchzuführende Aktion bei infizierten Dateien** können Sie festlegen, welche Aktion beim Feststellen einer infizierten Datei automatisch durchgeführt werden soll. Wählen Sie eine der folgenden Aktionen aus:

Aktion	Beschreibung
Nach Scannen fragen	Der Desinfektions-Assistent wird gestartet, wenn eine infizierte Datei festgestellt wird.
Automatisch desinfizieren	Die Datei wird automatisch desinfiziert, wenn ein Virus festgestellt wird.
Automatisch umbenennen	Die Datei wird automatisch umbenannt, wenn ein Virus gefunden wird.
Automatisch löschen	Die Datei wird automatisch gelöscht, wenn ein Virus gefunden wird. Diese Option ist nicht empfehlenswert, da dadurch die Datei, an die der Virus angehängt wurde, ebenfalls gelöscht wird.
Nur Bericht	Gibt an, dass ein Virus festgestellt wurde, und verhindert, dass das infizierte Objekt geöffnet wird. Bei Auswahl dieser Option werden Viren nur gemeldet, es wird aber keine Aktion ausgeführt.

4.6 Schutzeinstellungen zum Ignorieren/Scannen ausgewählter Dateien aktivieren

In bestimmten Fällen ist es ratsam, den Virenschutz einzustellen, um bestimmte Dateitypen bzw. bestimmte Dateien zu ignorieren. Beispielsweise, wenn Folgendes der Fall ist:

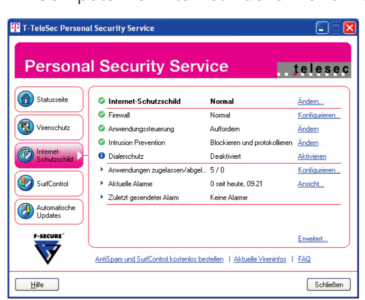
- Sie sind sicher, dass eine Datei nicht infiziert ist und ein falscher Alarm vorliegt.
- Ihr Computer ist weitgehend ausgelastet, und das Einstellen des Virenschutzes auf das Scannen aller Dateien würde die Arbeitsprozesse Ihres Computers erheblich verlangsamen und so ein Arbeiten unmöglich machen.
- Die Datei hat einen Dateityp, der nie durch Viren infiziert wird. Bei einigen Profilen sind die Scan-Einstellungen bereits so eingestellt, dass nur bestimmte Dateitypen gescannt werden. Dadurch wird gewährleistet, dass hauptsächlich Dateien gescannt werden, die üblicherweise von Viren infiziert werden, so dass der Prozessor und Speicher nicht unnötig belegt werden.

Warnung: Wenn der Virenschutz darauf eingestellt wird, bestimmte Dateien zu ignorieren, bedeutet dies, dass diese Dateien für zukünftige Virusangriffe anfällig sind und der Virusscan Viren unter Umständen nicht finden oder desinfizieren kann. Dies wird nur empfohlen, wenn es zwingend notwendig ist.

5. Internet-Schutzschild



Der Internet-Schutzschild überwacht und filtert den Netzwerkdatenverkehr und schützt so Ihren Computer vor unbefugten Zugriffen aus dem Internet. Darüber hinaus wird Ihr Computer vor Internet-Hackern und Netzwerkwürmern verborgen.



Option	Beschreibung
Internet-Schutzschild	Zeigt den Status des Internet-Schutzschilds an. Klicken Sie mit der rechten Maustaste auf **Ändern ...,** um die Sicherheitsstufe für den Internet-Schutzschild anzuzeigen und zu ändern. Wählen Sie eine Sicherheitsstufe, um die entsprechende Beschreibung anzuzeigen. Klicken Sie anschließend auf **OK,** um die Sicherheitsstufe zu verwenden, oder klicken Sie auf **Abbrechen,** um die aktuelle Sicherheitsstufe beizubehalten.
Firewall	Zeigt den Status der Firewall an. Klicken Sie auf **Konfigurieren ...,** um die Regeln und Einstellungen für die Firewall zu konfigurieren.
Anwendungssteuerung	Zeigt den aktuellen Status der Anwendungssteuerung an. Klicken Sie auf **Ändern ...,** um den Status der Anwendungssteuerung zu ändern. Sie haben die Auswahl zwischen **Auffordern** und **Zulassen und protokollieren.** Wir empfehlen Ihnen **Auffordern,** damit Sie immer ein Fenster mit einer Information erhalten und entscheiden können, ob Anwendungen zugelassen oder abgelehnt werden sollen. Die Anwendungen generell zuzulassen, ist nicht empfehlenswert.

Option	Beschreibung
Intrusion Prevention	Zeigt den Status von Intrusion Prevention an. Klicken Sie auf **Ändern ...,** um den Status von Intrusion Prevention zu ändern. Sie haben die Auswahl zwischen **Blockieren und protokollieren** und **Nur protokollieren.** Wir empfehlen Ihnen **Blockieren und protokollieren,** damit Sie einen Schutz vor Netzwerkangriffen haben. Falls Sie **Nur protokollieren** auswählen, wird zwar alles aufgezeichnet, aber die Gefahr bleibt bestehen.
Dialerschutz	Zeigt den Status des Dialerschutzes an. Klicken Sie auf **Ändern,** um den Status des Dialerschutzes zu ändern. Wenn Sie nicht via DSL ins Internet gehen, sollte der Dialerschutz auf **Aktiviert** stehen. Indem Sie mit der linken Maustaste auf **Aktivieren** oder **Deaktivieren** klicken, können Sie den Status des Dialerschutzes ändern. Bei Analog- oder ISDN-Verbindungen zum Internet via DFÜ wird nicht empfohlen, den Dialerschutz zu deaktivieren.
Anwendungen zugelassen/ abgelehnt	Überprüfen Sie, wie viele Anwendungen Verbindungen zum Internet aufbauen dürfen und wie viele gesperrt sind. Wenn Sie die Verbindungsrechte einer Anwendung ändern möchten, klicken Sie auf **Konfigurieren ...**
Aktuelle Alarme	Zeigt an, wie viele Alarme Sie in der letzten Zeit erhalten haben. Klicken Sie auf **Ansicht ...,** um die Liste mit den Alarmen anzuzeigen.
Zuletzt gesendeter Alarm	Zeigt die Uhrzeit des letzten Alarms an. Klicken Sie auf **Details ...,** um Informationen zum letzten Alarm sowie die fünf am häufigsten blockierten Protokolle und Hosts (IP-Adressen) anzuzeigen.

Der Internet-Schutzschild funktioniert nur, wenn TCP/IP installiert ist. Ein Ethernet-Adapter, DFÜ-Adapter, ISDN-, ADSL- oder HDSL-Adapter ist erforderlich. Token-Ring-Netzwerkadapter werden nicht unterstützt. Der Internet-Schutzschild filtert nur den IP-Datenverkehr, d. h., anderer, nicht auf IP basierender Datenverkehr wird ohne Filtervorgänge durchgelassen.

5.1 Erweiterte Einstellungen

Auf der Statusseite des Internet-Schutzschildes können Sie unter **Erweitert** die zur Verfügung stehenden Funktionen aktivieren und deaktivieren. Um Einstellungen der einzelnen Funktionen vorzunehmen, müssen Sie links im Verzeichnisbaum auf die jeweiligen Komponenten klicken.

Option	Beschreibung
Internet-Schutzschild	Zeigt den Status des Internet-Schutzschilds an. Klicken Sie auf die Auswahl, in dem der Name der bisherigen Sicherheitsstufe steht. Wenn Sie die Sicherheitsstufe ändern wollen, wählen Sie eine neue Sicherheitsstufe und klicken Sie im Anschluss auf **Anwenden.**
Firewall	Zeigt den Status der Firewall an. Im Normalfall sollte die Firewall auf **Aktiviert** stehen. Indem Sie mit der linken Maustaste auf **Aktivieren** oder **Deaktivieren** klicken und die Änderung mit **OK** bestätigen, können Sie den Status der Firewall ändern. Es wird nicht empfohlen, die Firewall zu deaktivieren.
Anwendungs-steuerung	Zeigt den Status der Anwendungssteuerung an. Im Normalfall sollte die Anwendungssteuerung auf **Aktiviert** stehen. Indem Sie mit der linken Maustaste auf **Aktivieren** oder **Deaktivieren** klicken, können Sie den Status der Anwendungssteuerung ändern. Es wird nicht empfohlen, die Anwendungssteuerung zu deaktivieren.
Intrusion Prevention	Zeigt den Status von Intrusion Prevention an. Im Normalfall sollte Intrusion Prevention auf **Aktiviert** stehen. Indem Sie mit der linken Maustaste auf **Aktivieren** oder **Deaktivieren** klicken, können Sie den Status von Intrusion Prevention ändern. Es wird nicht empfohlen, Intrusion Prevention zu deaktivieren.
Dialerschutz	Zeigt den Status des Dialerschutzes an. Wenn Sie nicht via DSL ins Internet gehen, sollte der Dialerschutz auf **Aktiviert** stehen. Indem Sie mit der linken Maustaste auf **Aktivieren** oder **Deaktivieren** klicken, können Sie den Status des Dialerschutzes ändern. Bei Analog- oder ISDN-Verbindungen zum Internet via DFÜ wird nicht empfohlen, den Dialerschutz zu deaktivieren.
Sicherheitsstufe für den Internet-Schutzschild	Zeigt die zurzeit ausgewählte Sicherheitsstufe an. Wenn Sie die Sicherheitsstufe ändern möchten, klicken Sie mit der linken Maustaste auf den Pfeil des Auswahlfeldes. Anschließend werden Ihnen alle zur Auswahl stehenden Sicherheitsstufen angezeigt. Wählen Sie sich zunächst die Beschreibung der Stufen durchlesen und anschließend eine neue Stufe auswählen, indem Sie mit der linken Maustaste auf den jeweiligen Namen klicken und den Button **Anwenden** drücken.

Die Paketfilterung bildet die Hauptfunktion des Internet-Schutzschildes; wenn Sie diese Funktion deaktivieren, ist der Internet-Schutzschild größtenteils unwirksam gegenüber allen Arten von Netzwerkangriffen.

Hinweis: Dieser Abschnitt richtet sich nur an erfahrene Computerbenutzer. Der Internet-Schutzschild kann durch Änderung von Einstellungen deaktiviert werden.

5.2 Sicherheitsstufe für den Internet-Schutzschild

Mit den Sicherheitsstufen für den Internet-Schutzschild können Sie Ihre Schutzstufe jederzeit an Ihre Anforderungen anpassen. Durch automatische Updates wird darüber hinaus sichergestellt, dass Sie vor den neuesten Arten von bösartigen Computer-Programmen und Internet-Angriffen geschützt sind.

5.2.1 Ändern der Sicherheitsstufe für den Internet-Schutzschild

Der Internet-Schutzschild verfügt über vordefinierte Sicherheitsstufen, die den gesamten Datenverkehr zulassen oder sperren, sowie eine Stufe, mit der Sie eigene benutzerdefinierte Regeln erstellen können. Darüber hinaus gibt es automatisch angepasste Sicherheitsstufen, bei denen einige Regeln nicht geändert werden können. Sie können die Einstellungen für die Sicherheitsstufen jederzeit an den erforderlichen Schutz anpassen. Durch das Ändern der ausgewählten Sicherheitsstufe wird die Stufe für automatisierte Vorgänge und Berichtsfunktionen geändert. Wählen Sie die gewünschte Sicherheitsstufe aus der Dropdown-Liste im Dialogfeld **Sicherheitsstufe für Internet-Schutzschild** aus. Lesen Sie die Beschreibung der jeweiligen Sicherheitsstufe aufmerksam durch, bevor Sie die Sicherheitsstufe aktivieren. Klicken Sie auf **OK,** um die ausgewählte Sicherheitsstufe zu verwenden.

5.3 Alarmmeldungen des Internet-Schutzschilds

Auf der Registerkarte **Alarme** werden alle Alarme des Internet-Schutzschilds aufgeführt. Sie können detaillierte Informationen zu einem Alarm anzeigen. Doppelklicken Sie dazu auf den Alarm oder markieren Sie ihn, und klicken Sie auf **Eigenschaften ...,** oder klicken Sie mit der rechten Maustaste auf den Alarm, und wählen Sie **Eigenschaften** aus dem Kontextmenü. Klicken Sie mit der rechten Maustaste auf einen einzelnen Alarm und wählen Sie **Löschen** aus dem Kontextmenü, um diesen Alarm zu entfernen. Klicken Sie auf **Alle löschen,** wenn Sie sämtliche Einträge aus der Alarm-

liste entfernen möchten. Wenn bei jedem Auftreten eines Alarms oder auf Grund einer von Ihnen erstellten Regel ein Pop-up-Fenster eingeblendet werden soll, aktivieren Sie das Kontrollkästchen **Dialogfeld Alarm anzeigen.**

Kennzeichnung der Alarmmeldungen:

Rot Attacken unterschiedlicher schädlicher Software (Malware), wie Trojaner usw.

Gelb Ungültiges Datenpaket bzw. Segment

Blau Blockierter Verkehr, der z. B. durch eine aktive Firewall-Regel gesperrt wird

5.3.1 Alarmeigenschaften

Wenn Sie auf einen Alarm doppelklicken oder einen Alarm markieren und anschließend auf **Eigenschaften** klicken, wird das Dialogfeld **Alarmeigenschaften** geöffnet. Hier werden der Alarmkommentar (der beim Erstellen der Regel eingegeben wurde, die den Alarm ausgelöst hat) sowie die IP-Adresse des betroffenen Remote-Computers und die Uhrzeit des Alarms angezeigt. Außerdem werden die Richtung des Datenverkehrs und die ausgeführte Aktion angezeigt. Des Weiteren finden Sie Angaben zum betroffenen Protokoll und zu den Ports sowie dem verwendeten Dienst, sofern diese Informationen ermittelt werden können.

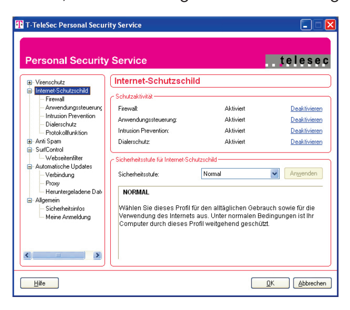
Alarminformationen	
Zeitstempel	Datum und Uhrzeit des Alarms.
Beschreibung	Der Alarmkommentar, der zusammen mit der Regel festgelegt wurde, die den Alarm ausgelöst hat.
Aktion	Gibt an, ob der Internet-Schutzschild die Anwendung, die den Alarm ausgelöst hat, zugelassen oder abgelehnt hat.
Richtung	Gibt an, ob es sich um eingehenden oder ausgehenden Datenverkehr handelt.
Protokoll	IP-Protokoll des Pakets.
Dienste für diese Verbindung oder Regel	Zeigt die übereinstimmenden Dienste für das Paket an, das den Alarm ausgelöst hat.

Host-Informationen	
Remote-Port	Der Port der Remote-Adresse, von dem das Paket gesendet oder empfangen wurde.
Lokaler Port	Der lokale Netzwerk-Port, von dem das Paket gesendet oder empfangen wurde.
Remote-Adresse	Die Remote-IP-Adresse des Pakets, das den Alarm ausgelöst hat.
Lokale Adresse	Die lokale IP-Adresse des Pakets, das den Alarm ausgelöst hat. Dabei handelt es sich entweder um eine Unicast-Adresse, eine Multicast-Gruppe oder eine Rundruf-Adresse.

Klicken Sie auf **DNS-Name,** um den aus der IP-Adresse aufgelösten DNS-Namen anzuzeigen, wenn dies möglich ist. Klicken Sie auf **Vor** oder **Weiter,** um zum vorherigen oder nächsten Alarm in der Liste zu wechseln. Klicken Sie auf **OK,** um das Eigenschaftsfenster **Alarme** zu schließen.

5.3.2 Zuletzt gesendeter Alarm

Im Dialogfeld **Zuletzt gesendeter Alarm** wird eine Zusammenfassung der letzten Warnmeldungen in Ihrem System angezeigt. Neben der genauen Uhrzeit des letzten Alarms sowie der IP-Adresse des betreffenden verdächtigen Datenpakets wird der Dienst angezeigt, der den Alarm ausgelöst hat. Darüber hinaus sehen Sie die Anzahl der Alarme, die seit der letzten Überprüfung empfangen wurden. Angezeigt werden auch eine Liste der fünf Dienste, die am häufigsten blockiert wurden, und der fünf Hosts, die am häufigsten Alarme ausgelöst haben.



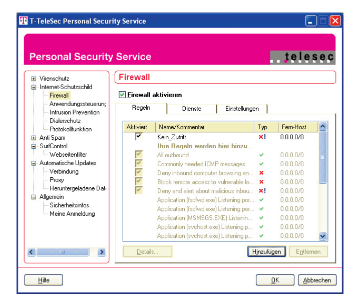
5.4 Anpassen von Internet-Schutzschild-Regeln

In einigen Situationen kann es erforderlich sein, dass Sie Regeln, die die Vorgehensweise bei bestimmten Verbindungen definieren, hinzufügen, ändern bzw. löschen möchten. Dieser Fall kann bei folgenden Vorgängen eintreten:

- Verbindungsherstellung zu einem neuen Spiele-Server auf einem bestimmten Computer
- Zulassen allgemeiner Verbindungen, aber Blockieren einer Verbindung zu einer bestimmten Webseite bzw. einem Computer, der/dem Sie nicht vertrauen

So passen Sie die Einstellungen Ihres Internet-Schutzschildes an:

1. Klicken Sie auf der Seite Internet-Schutzschild auf **Konfigurieren.** Das Fenster zu den Firewall-Einstellungsmöglichkeiten wird angezeigt.
2. Wählen Sie die entsprechende Registerkarte **Regeln, Dienste** oder **Einstellungen,** die Sie für Ihre Änderungen benötigen, aus.



3. Klicken Sie z. B. auf die Registerkarte **Regeln.**
   - Um eine bereits bestehende Regel zu ändern, wählen Sie diese aus der Liste aus und klicken Sie auf **Details.**
   - Um eine neue Regel hinzuzufügen, klicken Sie auf **Hinzufügen.**
   - Um eine Regel zu löschen, wählen Sie diese aus der Liste aus und klicken Sie auf **Entfernen.**

Hinweis: Vordefinierte Regeln können nicht geändert bzw. gelöscht werden. Sie können nur neue Regeln hinzufügen bzw. von Ihnen selbst hinzugefügte Regeln ändern und löschen.

5.4.1 Erstellen von neuen Internet-Schutzschild-Regeln

Schritt 1: Regeltyp.
Geben Sie der Regel einen beschreibenden Namen, und lassen Sie entweder die Verbindung zu oder lehnen Sie diese ab. Des Weiteren können Sie mit Hilfe des Kontrollkästchens festlegen, ob diese Regel nur auf DFÜ-Verbindungen angewendet werden soll.

Schritt 2: Wählen Sie aus, ob Sie diese Regel auf alle Verbindungen oder nur auf bestimmte Verbindungen anwenden möchten. Geben Sie dazu Ziele (IP-Adresse des Hosts/der Netzwerke oder bestimmte Adressbereiche) für diese Regel ein.
Sie haben folgende Möglichkeiten:

- Aktivieren Sie **Beliebige IP-Adresse,** um die Regel für alle Internetverbindungen anzuwenden, und klicken Sie auf **Weiter,** um mit Schritt 3 fortzufahren.
  Deaktivieren Sie **Beliebige IP-Adresse** und klicken Sie auf **Bearbeiten,** um ein neues Fenster zu öffnen, in dem Sie die Zieldetails eingeben können.
- Die Ziele können in beliebiger Reihenfolge und unabhängig vom Typ aufgeführt werden; das Ziel kann entweder ein DNS-Name, eine IP-Adresse, ein Teilnetz (im Bit-Netzmaskenformat) oder ein IP-Adressen-Bereich sein.
  Beispielsweise:
  DNS-Name www.some.domain.org
  IP-Adresse 192.168.5.16
  Teilnetz 192.168.88.0/29
  IP-Bereich 192.168.1.1-192.168.1.63

Klicken Sie auf die Schaltfläche **Zur Liste hinzufügen,** um das neue Ziel in die Liste der Ziele aufzunehmen, auf die diese Regel angewandt werden soll. Um ein Ziel aus der Liste zu entfernen, wählen Sie es aus und klicken Sie dann auf **Entfernen.** Um die Eigenschaften eines Ziels zu bearbeiten, wählen Sie aus der Liste die Zieladresse aus. Klicken Sie auf **OK,** um zur Seite 2/5 zu wechseln, und klicken Sie dann auf **Weiter,** um fortzufahren.

Schritt 3: Wählen Sie den Dienst und die Richtung für die Regel aus.

Bestimmen Sie nun aus der Liste der verfügbaren Dienste den Dienst, für den diese Regel angewendet werden soll. Wenn die Regel auf alle Dienste angewendet werden soll, wählen Sie diese Einstellung aus der Liste die Option **All IP traffic** aus. Sie können beliebig viele Einzeldienste aussuchen. Wählen Sie für die ausgewählten Dienste die Richtung aus, in der die Regel angewendet wird, indem Sie auf das rote Fragezeichen klicken. Durch wiederholtes Klicken wechseln Sie zwischen den verfügbaren Optionen. In der unten stehenden Tabelle finden Sie einige Beispiele dazu.

Schritt 4: Wählen Sie die Protokoll- und Berichtsfunktion aus.

Sie können auswählen, ob Sie informiert werden möchten, wenn die Regel bei einem Verbindungsversuch angewendet wird. Sie können hier Ihre eigene Alarmmeldung erstellen. In der unten stehenden Tabelle finden Sie einige Beispiele dazu.

Option	Begriff	Erklärung
?	Undefiniert	Die Richtung wurde noch nicht definiert. Klicken Sie auf die Grafik, um eine Richtung zu definieren.
←	Eingehend	Der Dienst wird zugelassen/abgelehnt, wenn Ihr Computer diesen vom Internet erhält.
→	Ausgehend	Der Dienst wird zugelassen/abgelehnt, wenn Ihr Computer diesen ins Internet schickt.
↔	Beide	Der Dienst wird von Ihrem Computer aus in beide Richtungen zugelassen/abgelehnt.

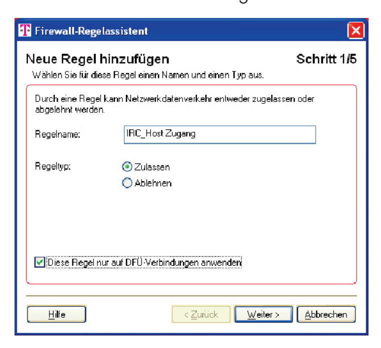
Schritt 5: Überprüfen und akzeptieren Sie die Regel.

Sie können jetzt Ihre Regel überprüfen. Klicken Sie auf **Zurück,** um an der Regel ggf. Änderungen vorzunehmen. Wenn die Regel Ihrer Zufriedenheit entspricht, klicken Sie auf **Fertig stellen.** Ihre neue Regel wird im aktiven Regelsatz in der **Registerkarte Regeln der Internet-Schutzschild-Einstellungen** zur Liste hinzugefügt.

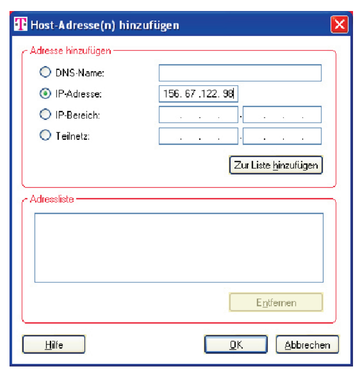
Beispiel: Erstellen einer Regel

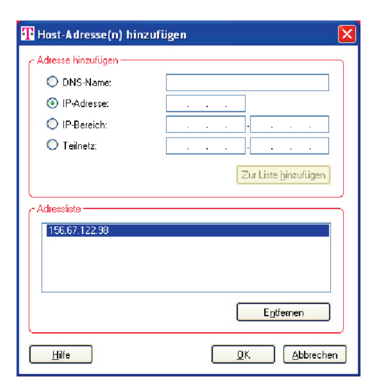
Der Zugriff auf einen bekannten IRC-Server soll über den definierten Dienst „IRC" über die nachfolgend eingerichtete Beispielregel ermöglicht werden.

1. Zunächst klicken Sie auf die Schaltfläche **Hinzufügen.**
2. Den Regelnamen, z. B. „IRC_Host Zugang", in das Feld **Regelname** eintragen und **Regeltyp zulassen** auswählen. Der Eintrag **nur auf DFÜ-Verbindungen anwenden** wird hier nicht aktiviert. (Dieser Eintrag ist in erster Linie für Sperr-Regeln, die nur bei aktiver DFÜ-Verbindung aktiv sein sollen, vorgesehen.) Danach die Schaltfläche **Weiter** betätigen.

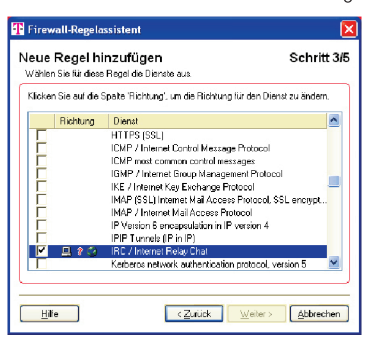


3. Nun wird die IP-Adresse des IRC-Servers eingetragen. Um diesen Zugang möglichst eng einzuschränken, sollte nicht der Eintrag **Beliebige IP-Adressen** ausgewählt werden, sondern die tatsächliche IP-Adresse des Servers eingetragen werden. Danach auf die Schaltfläche **Zur Liste hinzufügen** klicken und durch Betätigen der Schaltfläche **OK** die Eingabeseite abschließen.



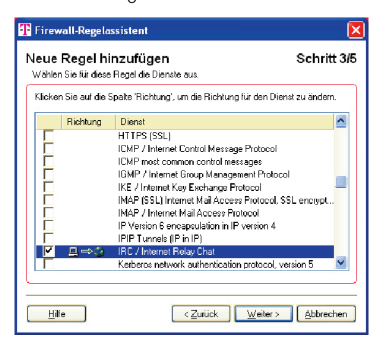


4. Durch Klicken der Schaltfläche **Weiter** gelangen Sie zum Dienste-Auswahlfenster.

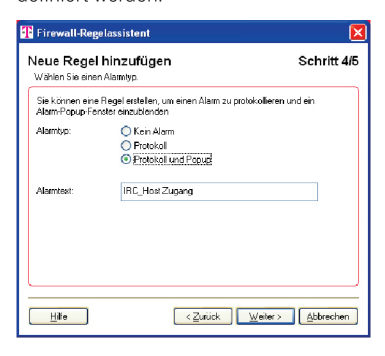


5. Hier wird der selbst definierte Dienst IRC durch einen Haken in der Auswahlbox ausgewählt.

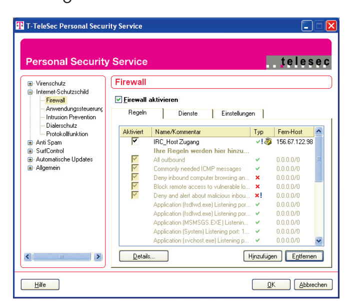
6. Durch mehrmaliges Klicken auf den Richtungspfeil wird die erlaubte Richtung für diesen Dienst festgelegt. Hier wird die Richtung ausgehend, also vom Host in das Internet, gewählt. Durch Klicken auf die Schaltfläche **Weiter** gelangen Sie zum nächsten Eingabefenster.



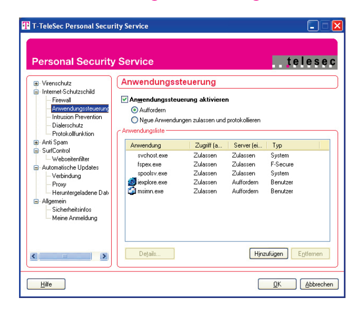
7. Im Fenster Alarm/Protokollierung kann zwischen den Optionen **Kein Alarm, Protokoll** und **Protokoll und Popup** ausgewählt werden. Es kann auch ein Alarmtext definiert werden.



8. Nach Betätigung der Schaltfläche **Weiter** werden alle Regelparameter noch einmal angezeigt. Durch Klicken auf die Schaltfläche **Fertig stellen** wird die Regel erzeugt und aktiviert.



5.5 Anwendungssteuerung



Vorgehensweise bei Anzeige des Pop-up-Fensters der Anwendungssteuerung

Wenn der Internet-Schutzschild installiert wurde, werden Sie von der Anwendungssteuerung gewarnt, wenn eine Anwendung versucht, eine Verbindung mit dem Internet herzustellen.

Hinweis: Anwendungen, die Sie nach der Installation schon im Startup-Assistenten als Standardanwendungen bestimmt haben, werden natürlich zugelassen, ohne eine Meldung anzuzeigen.

Bei der Anwendungssteuerung handelt es sich um ein Dienstprogramm, das alle Verbindungen zu oder von der Software zum Internet oder zu einem beliebigen lokalen Netzwerk überwacht. Abhängig von Ihren Einstellungen können Sie entweder alle Verbindungen zulassen und ein Protokoll der einzelnen Verbindungen erstellen. An-

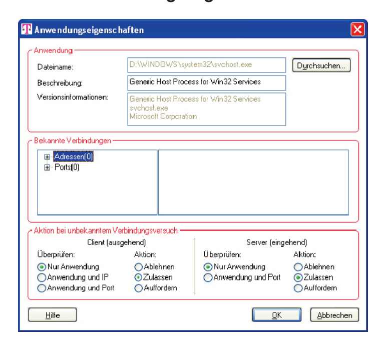
sonsten wird bei jedem Verbindungsversuch ein Fenster mit der Frage angezeigt, ob die Verbindung zugelassen werden soll. Außerdem wird überprüft, ob die Software, die einen Verbindungsaufbau versucht, mit der ursprünglich zugelassenen Software übereinstimmt. Wenn die Software geändert wurde, zeigt die Anwendungssteuerung eine entsprechende Warnung an und fragt den Benutzer, ob das geänderte Programm die Verbindung aufbauen darf oder nicht. Die Anwendungssteuerung gewährleistet sicheres Web-Browsing und ist eine hervorragende Verteidigung gegen schädliche Programme, wie z. B. Trojanische Pferde. Sie führt jedoch anfänglich zu einer Reihe von Aufforderungen zum Verhindern oder Zulassen von Verbindungen zu bestimmten Adressen. Die Zahl der Aufforderungen nimmt ab, und nach einiger Zeit werden nur noch selten Anwendungssteuerungs-Pop-ups angezeigt, es sei denn, Sie installieren neue Software, oder eine bösartige Anwendung versucht, eine Verbindung zwischen Ihrem Computer und dem Internet herzustellen. In der Anwendungsliste sehen Sie alle Anwendungen, die zugelassen und/oder abgelehnt werden sollen. Nach der Installation befinden sich in der Anwendungsliste Anwendungen, die vom Betriebssystem benötigt werden (z. B. bei Windows 2000 und XP: svchost.exe), sowie die Anwendung (fspex.exe), die es ermöglicht, automatisch nach Updates zu suchen und diese herunterzuladen. Auf der Seite **Anwendungssteuerung** können Sie die Berechtigungen für den ein- und ausgehenden Netzwerkdatenverkehr anzeigen, ändern und ergänzen. Aktivieren/Betätigen Sie das Kontrollkästchen **Anwendungssteuerung aktivieren,** um die Anwendungssteuerung einzuschalten. Wir empfehlen Ihnen die Anwendungssteuerung auf **Auffordern** zu stellen, falls die Anwendungssteuerung immer Ihre Genehmigung einholen soll, wenn eine Anwendung versucht, eine Verbindung zum Internet aufzubauen.
Über Anwendungsberechtigungen ist es nicht möglich, Datenverkehr zuzulassen, der auf Grund statischer Regeln gesperrt wurde. Wenn Sie jedoch bestimmte Arten von Netzwerkdatenverkehr über die statischen Regeln zugelassen haben, können Sie über die Anwendungssteuerung festlegen, ob die Zulassung durch die Regeln für die Anwendung gilt. Anders ausgedrückt: Sie können eine Regel erstellen, die Datenverkehr zulässt, und die Wirkung dieser Regel über die Anwendungssteuerung begrenzen. Die Anwendungssteuerung eignet sich hervorragend, um Trojaner (siehe Glossar, Trojanisches Pferd) und böswillige Netzwerk-Malware (schädliche Programme) abzuwehren, da sie nicht zulässt, dass diese Programme Informationen an das Netzwerk senden.

In der **Anwendungsliste** werden alle Anwendungen aufgeführt, deren Verbindungsversuche ins Netzwerk zugelassen oder gesperrt wurden.

- **Anwendung** zeigt den Dateinamen der Anwendung an.
- **Zugriff** (ausgehend) zeigt die aktuelle Aktion für ausgehende Verbindungen an, wenn die Anwendung versucht, eine Verbindung zum Netzwerk aufzubauen.
- **Server** (eingehend) zeigt die aktuelle Aktion für eingehende Verbindungen an, wenn ein Programm von außen versucht, eine Verbindung zur Anwendung im Netzwerk aufzubauen.
- **Typ** gibt an, ob die Regel manuell oder vom System erstellt wurde.

Mit einem Doppelklick auf die Anwendung können Sie deren Eigenschaften anzeigen oder die Anwendung auswählen. Klicken Sie dann auf **Details ...**

5.5.1 Anwendungseigenschaften



Im Fenster **Anwendungseigenschaften** werden die Eigenschaften einer Anwendung angezeigt. Sie können festlegen, ob Verbindungsversuche mit dem Netzwerk für die Anwendung zugelassen oder abgelehnt werden sollen. Ebenso können Sie festlegen, ob die Anwendung eingehende Verbindungsversuche annehmen darf oder ablehnen soll. Im Fenster **Anwendungseigenschaften** werden folgende Informationen angezeigt:

Anwendungsinformationen

Dateiname – Zeigt Pfad und Dateinamen der Programmdatei (.EXE) an. Achten Sie darauf, dass Pfad und Dateiname auf die richtige Anwendung verweisen. Über die Schaltfläche **Durchsuchen** können Sie eine andere ausführbare Datei (.EXE) auswählen.

Beschreibung – Zeigt die interne Beschreibung der ausführbaren Datei (.EXE) an. Normalerweise handelt es sich dabei um den Namen der Anwendung. Sie können die Beschreibung ändern.

Versionsinformationen – Zeigt die interne Versionsbeschreibung der ausführbaren Datei (.EXE) an.

Im Fensterbereich **Bekannte Verbindungen** werden die Adressen und Ports der Verbindungen angezeigt, die zugelassen oder gesperrt wurden. Sie können die Listen der zugelassenen und abgelehnten Adressen bearbeiten. Die Liste wird im rechten Fensterbereich angezeigt. Klicken Sie mit der rechten Maustaste auf den Eintrag im rechten Fensterbereich, um ihn zu bearbeiten. Sie können einen Eintrag aus einer Liste mit zugelassenen Adressen in eine Liste mit abgelehnten Adressen verschieben, oder Sie verschieben eine abgelehnte Adresse in die Liste der zugelassenen Adressen. Sie können Einträge löschen oder die IP-Adresse auflösen, um den **DNS-Namen** festzustellen.

Bekannte Verbindungen

Adressen	Ausgehend		Zugelassen	Besteht aus einer Liste aller ausgehenden IP-Adressen, zu denen die Anwendung eine Verbindung aufbauen darf.
Adressen	Ausgehend		Abgelehnt	Besteht aus einer Liste aller ausgehenden IP-Adressen, zu denen die Anwendung keine Verbindung aufbauen darf.
Ports	Ausgehend	TCP	Zugelassen	Besteht aus einer Liste aller ausgehenden TCP-Port-Nummern, zu denen die Anwendung eine Verbindung aufbauen darf.
Ports	Ausgehend	TCP	Abgelehnt	Besteht aus einer Liste aller ausgehenden TCP-Port-Nummern, zu denen die Anwendung keine Verbindung aufbauen darf.
Ports	Ausgehend	UDP	Zugelassen	Besteht aus einer Liste aller ausgehenden UDP-Port-Nummern, zu denen die Anwendung eine Verbindung aufbauen darf.
Ports	Ausgehend	UDP	Abgelehnt	Besteht aus einer Liste aller ausgehenden UDP-Port-Nummern, zu denen die Anwendung keine Verbindung aufbauen darf.
Ports	Eingehend	TCP	Zugelassen	Besteht aus einer Liste aller eingehenden TCP-Port-Nummern, zu denen die Anwendung eine Verbindung aufbauen darf.
Ports	Eingehend	TCP	Abgelehnt	Besteht aus einer Liste aller eingehenden TCP-Port-Nummern, zu denen die Anwendung keine Verbindung aufbauen darf.
Ports	Eingehend	UDP	Zugelassen	Besteht aus einer Liste aller eingehenden UDP-Port-Nummern, zu denen die Anwendung eine Verbindung aufbauen darf.
Ports	Eingehend	UDP	Abgelehnt	Besteht aus einer Liste aller eingehenden UDP-Port-Nummern, zu denen die Anwendung keine Verbindung aufbauen darf.

Über die Einstellungen in **Aktion bei unbekanntem Verbindungsversuch** können Sie entscheiden, welche Aktion ausgeführt werden soll, wenn die Anwendung versucht, mit den Einstellungen für den **Client (Ausgehend)** eine Verbindung zum Netzwerk aufzubauen, und wenn ein Programm von außen versucht, mit den Einstellungen für **Server (Eingehend)** eine Verbindung zu einer Anwendung im Netzwerk aufzubauen.

Folgende Aktionen sind möglich: Aktionen bei unbekannten Verbindungsversuchen

Überprüfen	
Nur Anwendung	Es wird nur überprüft, ob für diese Anwendung im Vorfeld eine ausgehende Verbindung zugelassen wurde. Bei einem positiven Ergebnis wird die Verbindung zugelassen. Andernfalls wird die ausgewählte Aktion ausgeführt.
Anwendung und IP	Es wird überprüft, ob für diese Anwendung im Vorfeld eine ausgehende Verbindung zugelassen wurde und ob die Verbindung für die angeforderte IP-Adresse zulässig ist. Wenn beide Bedingungen erfüllt sind, wird die Verbindung zugelassen. Andernfalls wird die ausgewählte Aktion ausgeführt. Wenn als **Aktion** die Option **Ablehnen** festgelegt wurde, wird die IP-Adresse in die Liste **Abgelehnt** aufgenommen. Wenn als Aktion die Option **Zulassen** festgelegt wurde, wird die IP-Adresse in die Liste **Zugelassen** aufgenommen.
Anwendung und Port	Es wird überprüft, ob für diese Anwendung im Vorfeld eine Verbindung zugelassen wurde und ob die Verbindung für den angeforderten Port zulässig ist. Wenn beide Bedingungen erfüllt sind, wird die Verbindung zugelassen. Andernfalls wird die ausgewählte Aktion ausgeführt. Wenn als **Aktion** die Option **Ablehnen** festgelegt wurde, wird die Port-Nummer in die Liste **Abgelehnt** aufgenommen. Wenn als **Aktion** die Option **Zulassen** festgelegt wurde, wird die Port-Nummer in die Liste **Zugelassen** aufgenommen.
Aktion	
Ablehnen	Die Verbindung wird abgelehnt, es sei denn, die Verifizierungsbedingungen wurden erfüllt, oder die IP-Adresse und die Port-Nummer befinden sich in der Liste **Zugelassen.**
Zulassen	Die Verbindung wird zugelassen, es sei denn, die Remote-IP-Adresse und die Port-Nummer befinden sich in der Liste **Abgelehnt.**
Auffordern	Bei jedem Verbindungsversuch mit dem Netzwerk wird ein Eingabefenster zum Festlegen der entsprechenden Aktion angezeigt, es sei denn, die Remote-Adresse oder der Netzwerk-Port befindet sich bereits auf den Listen **Abgelehnt** oder **Zugelassen.**
	IP-Adressen und Port-Nummern werden abhängig von den Verifizierungseinstellungen in die Listen der zugelassenen bzw. abgelehnten Adressen aufgenommen.

5.5.2 Was gilt als sichere Anwendung?

- Eine bekannte Anwendung, die Sie selbst aktiv gestartet haben
- Windows-Dienste, die keine Verbindung mit dem Internet herstellen

Sichere Microsoft-Windows-Dienste

Bei bestimmten Microsoft-Windows-Diensten ist zum Betrieb ein Netzwerkzugriff erforderlich. Die meisten Dienste werden automatisch zugelassen, die Anwendungssteuerung kann jedoch unter Umständen eine Eingabeaufforderung für die unten aufgeführten Dienste anzeigen; dies ist vor allem der Fall beim Betrieb auf Windows-NT-4.0-, Windows-2000- und Windows-XP-Plattformen. Lassen Sie bei diesen Plattformen den Zugriff auf das Netzwerk zu, da andernfalls einige der Windows-Funktionen nicht ausgeführt werden können.

Hier finden Sie die Anwendungen vor, die für die jeweiligen Betriebssysteme bereits als zugelassen in der Applikationskontrolle stehen:

Windows 98	Windows ME	Windows 2000	Windows XP	Bei allen Betriebssystemen
system\kernel32.dll system\msgsrv32.exe system\mprexe.exe pstores.exe	system\sspdsrv.exe explorer.exe	system32\lsass.exe system32\services.exe system32\svchost.exe system32\winlogon.exe system32\spoolsv.exe explorer.exe	system32\lsass.exe system32\svchost.exe system32\winlogon.exe system32\spoolsv.exe system32\alg.exe explorer.exe	system32\userinit.exe system32\ipconfig.exe winipcfg.exe ipconfig.exe sowie alle Anwendungen von Personal Security Service

Sie haben in der Anwendungsliste auch die Möglichkeit, Anwendungen manuell hinzuzufügen, zu entfernen und sich nähere Informationen zu den Anwendungen über den Button Details anzusehen.

5.5.3 Was gilt als unsichere Anwendung?

Anwendungen, die Sie von einer nicht vertrauenswürdigen Quelle empfangen haben, sollten immer mit Vorsicht behandelt werden. Anwendungen, die Sie von einer vertrauenswürdigen Quelle ohne vorherige Vereinbarung erhalten haben, sollten auch als verdächtig behandelt werden.

- Anwendungen, die Sie nicht selbst installiert haben oder die Ihnen unbekannt sind
- Anwendungen, die als sicher gelten, aber die versuchen, eine Verbindung herzustellen, ohne dass Sie sie starten
- Verbindungen, die keinen richtigen Zielnamen (Text-Webadresse) enthalten
- Fenster, die beim Surfen im Internet unerwartet und ungewollt angezeigt werden

5.5.4 Bestimmte Verbindungen zulassen und alle übrigen ablehnen

Führen Sie die folgenden Schritte aus, wenn Sie Verbindungen zu bestimmten IP-Adressen oder Ports zulassen und alle anderen Verbindungen ablehnen möchten:

1. Vergewissern Sie sich, dass die Liste der zugelassenen Adressen sämtliche IP-Adressen oder Port-Nummern enthält, zu denen Verbindungen aufgebaut werden können.
2. Ändern Sie die Einstellung für **Aktion** in **Ablehnen** und **Überprüfen** in **Nicht überprüfen.**

5.5.5 Bestimmte Verbindungen ablehnen und alle übrigen zulassen

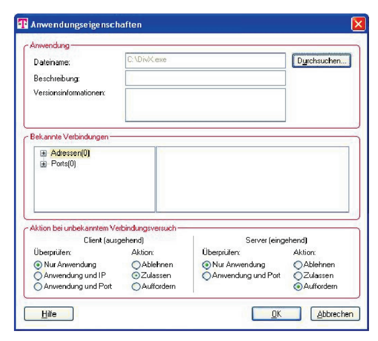
Führen Sie die folgenden Schritte aus, wenn Sie Verbindungen zu bestimmten IP-Adressen oder Ports ablehnen und alle anderen Verbindungen zulassen möchten:

1. Vergewissern Sie sich, dass die Liste der abgelehnten Adressen sämtliche IP-Adressen oder Port-Nummern enthält, zu denen keine Verbindungen möglich sein sollen.
2. Ändern Sie die Einstellungen für **Aktion** in **Zulassen** und **Überprüfen** in **Nicht überprüfen.**

Beispiel für das Hinzufügen einer neuen Applikation:

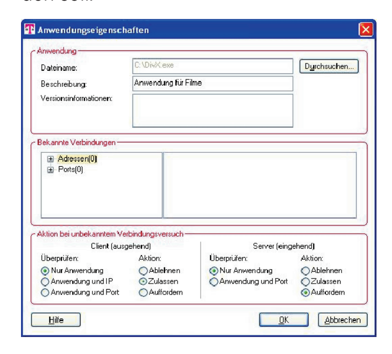
Schritt 1: Klicken Sie in der Anwendungsliste auf den Button **Hinzufügen.**

Schritt 2: Wählen Sie nun mit Hilfe des Buttons **Durchsuchen** die Anwendung auf Ihrem Rechner, die Sie ablehnen oder zulassen möchten. Sobald Sie diese mit **Öffnen** hinzugefügt haben, erscheinen in dem Feld **Dateiname** der Name und ggf. das Verzeichnis der Anwendung.



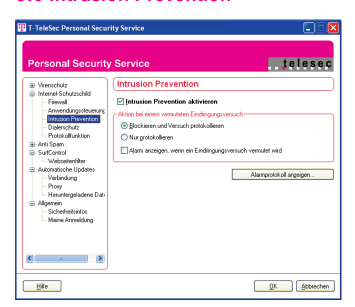
Schritt 3: Wenn Sie möchten, können Sie anschließend eine Beschreibung dieser Anwendung sowie Versionsinformationen in den entsprechenden Feldern hinterlegen.

Schritt 4: Zum Abschluss sollten Sie sich gründlich überlegen, welche Aktion bei unbekanntem Verbindungsversuch jeweils bei Client und Server durchgeführt werden soll.



Wenn Sie die Anwendungssteuerung deaktivieren möchten, rufen Sie die Seite für den Internet-Schutzschild auf. Klicken Sie neben der Anwendungssteuerung auf **Ändern.** Der Statustext wird von **Auffordern** in **Nur protokollieren** geändert.

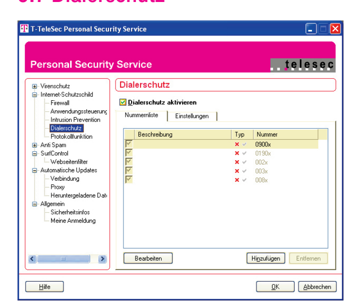
5.6 Intrusion Prevention



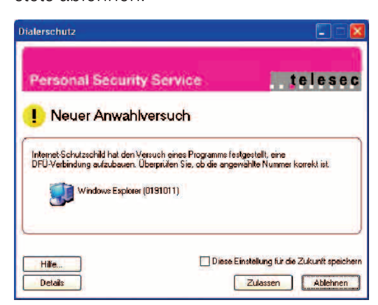
Bei Intrusion Prevention handelt es sich um eine Komponente des Internet-Schutzschilds, die den eingehenden Netzwerkdatenverkehr nach bestimmten Mustern überprüft, die auf einen laufenden Netzwerkangriff schließen lassen. Intrusion Prevention stellt einen zusätzlichen Schutz zu herkömmlichen Firewalls dar. Die Firewall legt in aller Regel Dienst, Port und Richtung der zugelassenen Internetverbindungen fest. Intrusion Prevention analysiert den gesamten Datenverkehr, um diesen nach Angriffsmustern zu untersuchen. Dazu gehören beispielsweise Port-Scans und Angriffe auf Ports, die von der Firewall nur ausgehend geöffnet sind. Diese werden häufig mit manipulierten Datenpaketen, die sich als Antwortpakete auf Aktionen des Hosts ausgeben, durchgeführt. Derartige Angriffe werden von Intrusion Prevention erkannt und geblockt.

Falls Intrusion Prevention bei Ihnen noch nicht aktiv ist, klicken Sie auf das Kontrollkästchen **Intrusion Prevention aktivieren,** um Intrusion Prevention zu aktivieren. Im Fensterbereich **Aktion bei einem vermuteten Eindringungsversuch** wählen Sie **Blockieren und Versuch protokollieren,** wenn der Eindringungsversuch blockiert werden soll. Wählen Sie **Nur protokollieren,** wenn vermutete Eindringungsversuche nur in einer Protokolldatei aufgezeichnet werden sollen. Aktivieren Sie das Kontrollkästchen **Alarm anzeigen, wenn ein Eindringungsversuch vermutet wird,** wenn bei einem vermuteten Eindringungsversuch ein Fenster mit einer Warnmeldung angezeigt werden soll. Klicken Sie auf **Alarmprotokoll anzeigen,** um eine Liste der letzten Warnmeldungen anzuzeigen.

5.7 Dialerschutz



Der Dialerschutz ist eine Funktion der Personal Firewall und schützt den Computer vor böswilligen Dialern, d.h. Programmen, die eine Verbindung zu einer kostenpflichtigen Service-Rufnummer (z.B. 0190/0900) aufbauen. Das Programm fängt alle auf Windows basierenden DFÜ-Verbindungsversuche ab. Anhand einer Liste mit zugelassenen und gesperrten Telefonnummern wird die Verbindung zugelassen oder abgelehnt, oder es wird ein Entscheidungsfenster angezeigt, in dem Sie darüber entscheiden, ob die Verbindung zugelassen werden soll. Wenn Sie den Verbindungsversuch nicht selbst eingeleitet haben, oder wenn Ihnen die Telefonnummer verdächtig erscheint, sollten Sie die Verbindung in dem unten eingefügten Entscheidungsfenster stets ablehnen.



Es ist nicht legitim, die Installation von Dialerprogrammen generell zu unterbinden. Deswegen verhindert die Dialerschutz-Funktion von Personal Security Service nicht die Installation der Dialerprogramme. Diese Programme können nur dann Schaden anrichten, wenn Sie die Verbindung zugelassen haben. Die Dialerschutz-Funktion von Personal Security Service schützt Sie vor unerwünschten Verbindungen. Sie selbst entscheiden, welche Dialer zugelassen oder abgelehnt werden sollen. Denn: Es gibt durchaus auch Dialerprogramme, die Sie ggf. verwenden möchten (z.B. für eine Rechts-

beratung). Personal Security Service überprüft nicht nur bestimmte Rufnummern (z.B. 0900-Nummern), sondern erkennt generell jeden Verbindungswunsch, egal welcher Rufnummer, und befragt Sie, ob Sie die Verbindung zulassen möchten oder nicht. Dadurch ist sichergestellt, dass alle Arten von Dialern, inkl. Auslandsdialern, erkannt werden. **Hinweis:** Neuerdings werden auch Verbindungswünsche erkannt, die über die CAPI- und TAPI-Schnittstelle hergestellt werden. Bislang wurden lediglich Verbindungsversuche erkannt, die über die Standard-DFÜ-Verbindung von Windows hergestellt wurden.

DSL und die Verwendung des Dialerschutzes

Eine DSL-Verbindung ist sozusagen eine Blockade für Dialerprogramme. DSL ist keine Wählverbindung, sondern eine Netzwerkverbindung. Das bedeutet, dass bei der Verbindungsherstellung nicht wie bei der herkömmlichen Internet-Einwahl über Analog-Modems oder ISDN-Karten gewählt wird, sondern hier wird der eigene Computer nur im DSL-Netzwerk des DSL-Providers angemeldet.

Warum wählt sich ein Dialer nicht über das DSL-Modem ein?

Der Splitter trennt die Signale in ein DSL-Signal (das zum DSL-Modem führt) und in ein Telefonsignal, zu dem auch die Internet-Einwahl über ein analoges Modem oder über eine ISDN-Karte zählt. Da der Dialer auf eine Wählverbindung angewiesen ist, scheitert er an der DSL-Schnittstelle, über die nur eine Netzwerkverbindung hergestellt werden kann. Die Dialerschutz-Funktion von Personal Security Service wacht auch über Verbindungsversuche, wenn Sie DSL verwenden und eine DFÜ-Verbindung auf Ihrem Computer eingerichtet haben, um z.B. Faxe zu versenden.

5.7.1 Dialerschutz-Protokollfunktion

Wenn eine Protokolldatei aller Verbindungsversuche erstellt werden soll, müssen Sie die Dialerschutz-Protokollfunktionen aktivieren. Gehen Sie auf der Hauptseite auf **Erweitert,** auf **Internet-Schutzschild** und anschließend auf **Dialerschutz** im Verzeichnisbaum. Um sich das Protokoll der Verbindungen anzeigen zu lassen, klicken Sie auf die Registerkarte **Einstellungen** und den Button **Protokoll anzeigen** (siehe Bild).

dial.log - Notepad

File Edit Format View Help

```
04/16/04 11:09:34,info,general,daemon,dial-up control logging enabled
04/16/04 11:31:26,info,general,daemon,dial-up control enabled
04/19/04 08:29:02,info,general,daemon,dial-up control logging enabled
04/19/04 08:29:08,info,dial-up control,daemon,0191011,allow,D:\PSS\FSGUI\FSSW.EXE
04/19/04 08:34:08,info,general,daemon,dial-up control disabled
04/19/04 08:47:37,info,general,daemon,dial-up control enabled
04/19/04 08:47:46,info,general,daemon,dial-up control disabled
04/19/04 08:47:50,info,general,daemon,dial-up control enabled
04/19/04 08:49:45,info,dial hang-up,daemon,allow,E:\WINDOWS\Explorer.EXE
04/19/04 08:49:45,info,duration,0:20:37
04/19/04 10:17:07,info,dial-up control,daemon,0191011,deny,E:\WINDOWS\Explorer.EXE
04/21/04 13:29:34,info,dial-up control,daemon,0191011,allow,E:\WINDOWS\Explorer.EXE
04/22/04 07:29:17,info,general,daemon,dial-up control logging enabled
04/22/04 07:30:52,info,dial-up control,daemon,0191011,allow,D:\PSS\FSGUI\FSSW.EXE
04/22/04 07:38:27,info,general,daemon,dial-up control disabled
04/25/04 17:02:31,info,general,daemon,dial-up control enabled
04/25/04 17:04:11,info,dial-up control,daemon,0191011,deny,D:\PSS\FSGUI\fssw.exe
04/25/04 17:23:25,info,dial-up control,daemon,0191011,allow,E:\WINDOWS\Explorer.EXE
04/25/04 17:23:36,info,dial hang-up,daemon,allow,E:\WINDOWS\Explorer.EXE
04/25/04 17:23:36,info,duration,0:00:11
04/28/04 07:19:02,info,dial-up control,daemon,0191011,allow,E:\WINDOWS\Explorer.EXE
07/23/04 09:15:17,info,general,daemon,dial-up control disabled
07/23/04 09:15:17,info,general,daemon,dial-up control logging enabled
07/23/04 09:33:08,info,general,daemon,dial-up control enabled
07/23/04 09:33:09,info,general,daemon,dial-up control disabled
07/24/04 18:07:51,info,general,daemon,dial-up control enabled
07/24/04 18:07:51,info,general,daemon,dial-up control disabled
07/24/04 18:07:52,info,general,daemon,dial-up control enabled
07/26/04 07:45:15,info,dial-up control,daemon,0191011,allow,E:\WINDOWS\Explorer.EXE
07/26/04 07:59:28,info,dial hang-up,daemon,allow,E:\WINDOWS\Explorer.EXE
07/26/04 07:59:28,info,duration,0:14:13
09/08/04 10:08:54,info,general,daemon,dial-up control disabled
09/15/04 09:46:11,info,general,daemon,dial-up control enabled
09/15/04 11:51:49,info,general,daemon,dial-up control disabled
```

Bitte beachten Sie, dass es in einigen Ländern gegen das Gesetz verstößt, Telefonnummern, die von anderen Teilnehmern gewählt wurden, ohne deren Wissen zu protokollieren.

5.7.2 Telefonnummern in der Dialerschutz-Liste anzeigen und bearbeiten

Gehen Sie wie folgt vor, um die Telefonnummern in der Liste anzuzeigen oder zu bearbeiten:

Schritt 1: Machen Sie einen Doppelklick auf das **T-Logo** in Ihrer Systemleiste neben der Uhranzeige.

Schritt 2: Klicken Sie anschließend auf den Button **Internet-Schutzschild** sowie auf **Erweitert.**

Schritt 3: Klicken Sie danach im Verzeichnisbaum auf **Dialerschutz.**

Schritt 4: Auf der Registerkarte **Nummernliste** wird eine Liste von Telefonnummern angezeigt, die für einen Verbindungsversuch zugelassen oder gesperrt sind. Bei einem neuen DFÜ-Verbindungsversuch werden die Nummern aus dieser Liste von oben nach unten überprüft, und die erste übereinstimmende Regel wird auf die Verbindung angewandt.

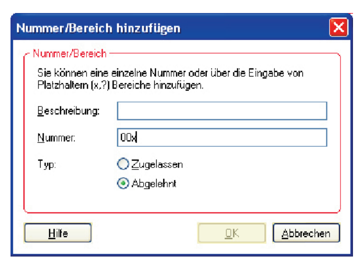
Hinweis: Der Dialerschutz hat bereits voreingestellte Rufnummern, die gesperrt sind. Mit Hilfe dieser eingetragenen Nummern können keine Verbindungen zu den bisher bekannten teuren Wählverbindungen aufgebaut werden. Diese Rufnummern lassen sich zu Ihrem Schutz nicht von Ihnen editieren.

Folgende Aktionen sind möglich:

- Um eine neue Nummer zur Liste hinzuzufügen, klicken Sie auf **Hinzufügen.**
- Um eine Nummer aus der Liste zu löschen, klicken Sie auf **Entfernen.**
- Um eine bereits bestehende Telefonnummer oder eine der Telefonnummer zugeordnete Aktion zu ändern, wählen Sie die Telefonnummer in der Liste mit Hilfe der linken Maustaste aus und klicken Sie auf **Bearbeiten.**
- Um eine Nummer in der Liste an einen höheren oder tieferen Rang zu verschieben, klicken Sie mit der rechten Maustaste auf die Telefonnummer und wählen Sie aus dem daraufhin erscheinenden Kontextmenü je nach Wunsch nach oben bzw. nach unten.

Eine neue Rufnummer zur Dialerschutz-Liste hinzufügen:

1. Klicken Sie auf **Hinzufügen.** Anschließend wird das Dialogfeld **Nummer/Bereich** geöffnet.

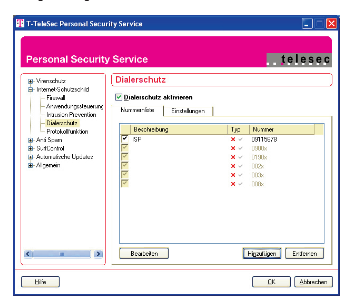


2. Geben Sie den Namen der Verbindung in das Feld **Beschreibung** ein.
3. Geben Sie anschließend die Rufnummer ein. Bitte geben Sie bei der Nummer die jeweilige Vorwahl ein.

Wenn Sie eine Regel definieren, die für mehrere Nummern gleichzeitig gilt, können Sie folgende Platzhalter verwenden:

- „?“, um eine einzelne Ziffer zu ersetzen
- „X“ (als Groß- oder Kleinbuchstaben) als Ersatz für eine beliebige Anzahl von Ziffern. Dieser Platzhalter eignet sich z. B. dafür, Verbindungen ins Ausland zu unterbinden. Wenn eine Auslandsverbindung normalerweise mit „00“ beginnt, können Sie „00X“ in das Feld Nummer eingeben, um eine Regel zu definieren, die für alle DFÜ-Verbindungsversuche zu einer ausländischen Telefonnummer gilt.

4. Wenn Sie DFÜ-Verbindungen zu dieser Nummer sperren möchten, aktivieren Sie das Kontrollkästchen **Abgelehnt,** um die Verbindungen zu dieser Nummer abzulehnen. Falls Sie diese Nummer explizit zulassen möchten, müssen Sie das Kontrollkästchen **Zulassen** auswählen.
5. Klicken Sie auf **OK,** um den Vorgang abzuschließen.
6. Die Telefonnummer und die zugeordnete Aktion werden daraufhin in der Liste angezeigt.

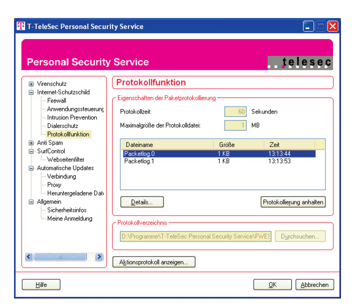


Hinweis: Es ist nicht möglich, die vordefinierten Einträge zu löschen. Aus diesem Grund werden die Einträge in der Liste für den Dialerschutz grau angezeigt. Sie können sie nur überschreiben, indem Sie Ihre eigene Regel für dieselbe Nummer oberhalb der ursprünglichen Regel in der Liste hinzufügen. Beispiel: Sie erstellen einen neuen Rufnummerneintrag in der Liste des Dialerschutzes, um einen vordefinierten Rufnummerneintrag außer Kraft zu setzen.

5.7.3 Einstellungen

Hier werden die Anwendungen angezeigt, die eine bestehende DFÜ-Verbindung trennen können. Wenn Sie möchten, können Sie diese in der Liste aufgeführten Anwendungen mit der rechten Maustaste einzeln auswählen und sie mit dem Button **Löschen** entfernen.

5.8 Protokollfunktion



Über die **Paketprotokollierung** und das **Aktionsprotokoll** können Sie fortlaufend Informationen über den Netzwerkverkehr und Aktionen des Internet-Schutzschilds aufzeichnen. Klicken Sie auf **Aktionsprotokoll anzeigen ...,** um das **Aktionsprotokoll** anzuzeigen.

5.8.1 Paketprotokollierung

Im **Paketprotokoll** werden detaillierte Informationen zum Netzwerkdatenverkehr aufgezeichnet. Aus diesem Grund ist diese Form der Protokollierung standardmäßig deaktiviert. Klicken Sie auf **Protokollierung starten,** um das Paketprotokoll zu aktivieren, wenn Sie schädliche Netzwerkaktivitäten vermuten. Nach Ablauf eines definierten Zeitraums oder bei Erreichen der Maximalgröße der Protokolldatei wird die Protokollfunktion automatisch angehalten. Klicken Sie auf **Protokollierung anhalten** um die Protokollfunktion manuell anzuhalten.

Das System verwaltet zehn verschiedene Paketprotokolldateien. Sie können daher vorherige Protokolle überprüfen, während ein neues Protokoll erstellt wird. Die Protokolldateien werden in einem binären Format gespeichert, das mit dem tcpdump-Format kompatibel ist. Sie können diese Dateien entweder mit dem Paketprotokoll-Viewer oder mit einem herkömmlichen Programm zur Paketprotokollierung anzeigen.

Der Paket-Logger protokolliert alle Arten des Netzwerkdatenverkehrs, einschließlich der vom LAN benötigten Protokolle, wie Routing-Informationen, Auflösungen der Hardware-Adressen usw. Diese Informationen sind in der Regel nicht besonders nützlich. Aus diesem Grund werden sie im integrierten Paketprotokoll-Viewer standardmäßig ausgeblendet. Wenn Sie diese Daten anzeigen möchten, deaktivieren Sie das Kontrollkästchen **Nicht-IP-Daten herausfiltern.**

5.8.2 Aktionsprotokoll

Im Aktionsprotokoll werden laufend Daten über die Aktivitäten des **Internet-Schutzschilds** gesammelt. Beim Aktionsprotokoll handelt es sich um eine normale Textdatei mit einer maximalen Größe von 10 MB. Sie können diese Datei mit jedem Texteditor öffnen und bearbeiten, der in der Lage ist, große Dateien zu lesen. Sie können Einträge aus der Aktionsprotokolldatei oder die gesamte Datei jederzeit löschen. Wenn die Datei zu groß wird, können Sie mühelos eine neue Datei für die Protokollierung anlegen. Der Pfad der Protokolldatei wird auf der Seite **Protokollfunktion** angezeigt.

Praktische Beispiele zum Lesen des Aktionsprotokolls:

5.8.3 Ändern einer Firewall-Richtlinie, z. B. Ändern der Sicherheitsstufe

11/16/02 15:48:01, Erfolgreich abgeschlossen, Allgemein, Daemon, Richtliniendatei wurde erneut geladen.

5.8.4 Öffnen einer eingehenden oder ausgehenden lokalen Verbindung

1	2	3	4	5	6	7	8	9	10
11/15/02	16:54:41	Info	appl control	C:\WINNT\system32\services.exe	Allow	Send	17	10.128.128.14	137

Beschreibung der Felder:

1. Datum
2. Zeit
3. Typ
4. Interner Grund
5. Name der Anwendung
6. Aktion der Anwendungssteuerung
7. Netzwerkaktion
8. Protokoll
9. Remote-IP
10. Remote-Port

5.8.5 Empfangende Verbindung

Wenn die Anwendung eine Verbindung aufgebaut hat, bei der sie einen bestimmten Port abhört, fungiert sie als Server. In diesem Fall können Remote-Computer eine Verbindung zu dem Port aufbauen, für den die Verbindung geöffnet wurde. Im Aktionsprotokoll werden diese Verbindungen ebenfalls aufgezeichnet (Protokollierung ist nach wie vor in Englisch).

1	2	3	4	5	6	7	8	9	10
11/15/02	16:48:00	Info	appl control	Unbekannt	Allow	Listen	17	10.128.129.146	138

Beschreibung der Felder:

1. Datum
2. Zeit
3. Typ
4. Interner Grund
5. Name der Anwendung
6. Aktion der Anwendungssteuerung
7. Netzwerkaktion
8. Protokoll
9. Remote-IP
10. Remote-Port

5.8.6 Eingabe einer dynamischen Regel

Wenn eine Anwendung eine Server-Verbindung aufbauen möchte, die Sie zulassen, wird diese Verbindung unter Umständen durch statische Firewall-Regeln verhindert. Aus diesem Grund wird diese eingehende Verbindung mit Hilfe einer dynamischen Verbindung zugelassen. Die dynamische Verbindung besteht dabei nur für die Dauer der Verbindung und gilt nur für diese Anwendungen.

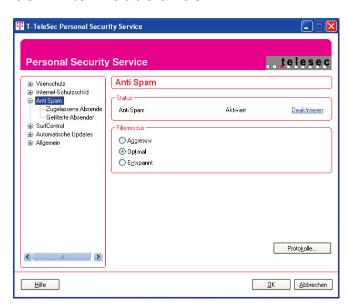
1	2	3	4	5	6	7	8	9	10	11	12
11/15/02	16:47:59	Info	Dynamische Regel	Hinzugefügt	0.0.0.0	255.255.255.0	0	65535	371	371	Zulassen
11/15/02	16:48:23	Info	Dynamische Regel	Entfernt	0.0.0.0	255.255.255.0	0	65535	371	371	Zulassen

Beschreibung der Felder:

1. Datum
2. Zeit
3. Alarmtyp
4. Regeltyp
5. Ausgeführte Aktion
6. Minimaler Adressbereich für Remote-IP
7. Maximaler Adressbereich für Remote-IP
8. Remote-Port-Bereich (Von)
9. Remote-Port-Bereich (Bis)
10. Lokaler Port-Bereich (Von)
11. Lokaler Port-Bereich (Bis)
12. Regelaktion (Zulassen/Ablehnen)

6. Anti Spam

Anti Spam überwacht eingehende E-Mails und entfernt unaufgefordert zugesandte Massen-E-Mails aus Ihrem Posteingang. Es setzt dabei heuristische Tests zur Identifikation von E-Mails als Spam ein. Wird eine E-Mail als Spam festgestellt, wird sie markiert und in einen separaten Spam-Ordner gefiltert. Wenn Sie überprüfen möchten, ob gültige E-Mails als Spams gefiltert wurden, öffnen Sie den Spam-Ordner und durchsuchen die Nachrichten in dem Ordner. Auf der Seite mit den **erweiterten Einstellungen für Anti Spam** können Sie Anti Spam aktivieren oder deaktivieren und den Filtermodus ändern.



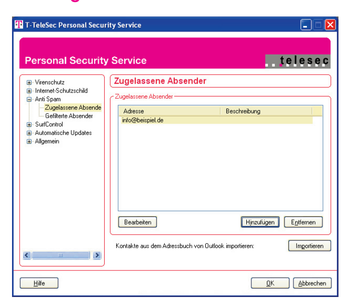
Option	Beschreibung
Anti Spam	**Aktiviert** oder **Deaktiviert.** Klicken Sie auf **Aktivieren/ Deaktivieren,** um Anti Spam ein- oder auszuschalten. Wenn Sie Anti Spam deaktivieren, werden alle Anti-Spam-Funktionen ausgeschaltet.
Filtermodus	**Aggressiv, Optimal** oder **Entspannt.** Wählen Sie die vordefinierte Stufe, um Spams zu filtern. Im Modus **Aggressiv** werden mehr Nachrichten von Anti Spam in den Spam-Ordner verschoben. Bei dieser Filtereinstellung kann es öfter dazu kommen, dass Mails, die nicht als Spam-Mails abgelegt werden sollen, als Spam-Mails definiert werden. Im Modus **Entspannt** werden weniger Nachrichten als Spam gefiltert. Auf diese Weise können Sie das Risiko minimieren, dass legale Nachrichten versehentlich in den Spam-Ordner verschoben werden.

Option	Beschreibung
Protokolldatei anzeigen	Öffnet eine Protokolldatei mit Informationen zu allen gelöschten E-Mails.
Protokolle	Sie können die TCP/IP-Ports für die E-Mail-Protokolle POP3, IMAP4 und SMTP konfigurieren. Standardmäßig verwendet das Programm die Standard-Ports.

6.1 Funktionsweise von Anti Spam und Filtermodus

Anti Spam untersucht die eingehenden Mails hinsichtlich Spam mit zwei unterschiedlichen Filtern. Dabei werden sowohl der E-Mail-Header als auch der Inhalt von einem statischen und einem dynamischen, also lernfähigen Filter durchsucht. Dabei wird nach Merkmalen gesucht, die typisch für Massenmails sind (z. B. große Empfänger-Verteiler und bestimmte Marketingbegriffe). Jeder Filter gibt eine Bewertung hinsichtlich der Wahrscheinlichkeit, dass es sich bei dieser Nachricht um Spam handelt, ab. Als Ergebnis dieser Untersuchung erhält die Nachricht eine Gesamtbewertung zwischen 0 und 7, wobei der Verdacht, dass es sich um Spam handelt, bei der Bewertung 7 am höchsten ist. Mit Hilfe des Filtermodus kann der Benutzer nun den Grenzwert bestimmen, ab dem eine Mail in den Spamordner verschoben wird. Bei der „großzügigsten“ Stufe **Entspannt** werden Mails erst ab einer Bewertung von 7 in den Spam-Ordner verschoben. Die Wahrscheinlichkeit, dass auch Spam im Posteingang abgelegt wird, wird dadurch höher. Im Filtermodus **Optimal** liegt der Grenzwert bei 5, im Filtermodus **Aggressiv** bei 3. Hier ist es weitgehend ausgeschlossen, dass Spam im Posteingang abgelegt wird, allerdings ist auch nicht ausgeschlossen, dass ggf. auch andere E-Mails als Spam interpretiert werden.

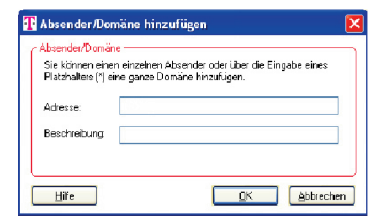
6.2 Zugelassene Absender



Die Liste der zugelassenen Absender enthält Adressen, die nicht gefiltert und in den Spam-Ordner verschoben werden sollen. Sie können E-Mail-Adressen einzeln oder als Gruppen zur Liste der zugelassenen Absender hinzufügen. Beispiel: Über den Eintrag *@beispiel.com lassen Sie alle E-Mails aus der Domäne beispiel.com zu.

6.2.1 Hinzufügen und Entfernen von Adressen

1. Klicken Sie auf **Hinzufügen ...,** um eine neue E-Mail-Adresse zur Liste hinzuzufügen.
2. Geben Sie die Adresse in die Adresszeile ein. Sie können wahlweise eine kurze Beschreibung der neuen Adresse in das Feld **Beschreibung** eingeben. Klicken Sie auf **OK,** um die neue E-Mail-Adresse in die Liste aufzunehmen.



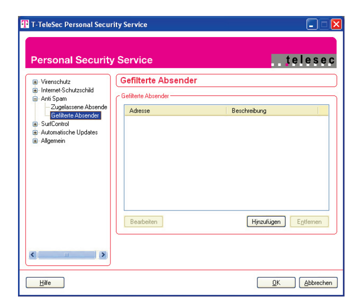
Sie können nun auch einen zuvor angelegten Eintrag bearbeiten. Wählen Sie dazu eine Adresse aus, und klicken Sie auf **Bearbeiten ...,** um die Änderungen vorzunehmen. Klicken Sie auf **Entfernen,** um die ausgewählte Adresse zu entfernen.

Wenn Sie eine neue Adresse hinzufügen möchten, klicken Sie in Microsoft Outlook auf die Menüschaltfläche **Anti Spam.** Wählen Sie die Nachricht aus und wählen Sie anschließend **Absender zulassen,** um die Adresse des Absenders in die Liste der zugelassenen Absender aufzunehmen.

6.2.2 Importieren von Kontakten

Sie können die Adressen aus der Kontaktliste von Microsoft Outlook in die Liste der zugelassenen Absender importieren. Klicken Sie mit der linken Maustaste auf **Importieren,** um die Kontakte in die Liste der zugelassenen Absender zu importieren. Nachdem Sie alle Kontakte importiert haben, können Sie Adressen bearbeiten und entfernen. Falls keine Einträge in Ihren Outlook-Kontakten abgespeichert sind, erscheint die Fehlermeldung **Es wurden keine Adressen für den Import gefunden.**

6.3 Gefilterte Absender



Die Liste der gefilterten Absender enthält Adressen, die herausgefiltert und in den Spam-Ordner verschoben werden sollen. Die Liste kann einzelne E-Mail-Adressen oder Adressgruppen enthalten. Beispiel: Über den Eintrag *@beispiel.com filtern Sie alle E-Mails aus der Domäne beispiel.com.

6.3.1 Hinzufügen und Entfernen von Adressen

1. Klicken Sie auf **Hinzufügen ...,** um eine neue E-Mail-Adresse zur Liste hinzuzufügen.
2. Geben Sie die Adresse in die Adresszeile ein. Sie können wahlweise eine kurze Beschreibung der neuen Adresse in das Feld **Beschreibung** eingeben. Klicken Sie auf **OK,** um die neue E-Mail-Adresse in die Liste aufzunehmen.

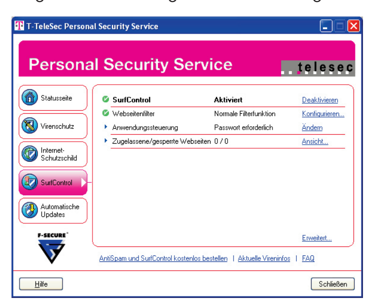
Sie können einen zuvor angelegten Eintrag bearbeiten:
Wählen Sie dazu eine Adresse aus, und klicken Sie auf **Bearbeiten ...,** um die Änderungen vorzunehmen. Klicken Sie auf **Entfernen,** um die ausgewählte Adresse zu entfernen.

Wenn Sie eine neue Adresse hinzufügen möchten, klicken Sie in Microsoft Outlook auf die Menüschaltfläche **Anti Spam.** Wählen Sie die Nachricht aus, und wählen Sie anschließend **Absender filtern,** um die Adresse des Absenders in die Liste der gefilterten Absender aufzunehmen.

7. SurfControl



Mit Hilfe der SurfControl können Sie unerwünschte Webseiten blockieren und den Zugriff auf die Programmeinstellungen einschränken.



Hinweis: Im Microsoft Internet Explorer wird SurfControl in Form einer Schaltfläche in die Symbolleiste integriert . Über diese Schaltfläche können Sie Webseiten zulassen oder sperren und den Webseitenfilter vorübergehend aussetzen.

Option	Beschreibung
SurfControl	**Aktiviert** oder **Deaktiviert.** Wenn Sie SurfControl deaktivieren, werden ALLE Funktionen von SurfControl so lange ausgeschaltet, bis Sie sie erneut aktivieren. Wenn Sie SurfControl vorübergehend deaktivieren möchten, klicken Sie auf das Symbol neben der Uhranzeige auf Ihrem PC mit der rechten Maustaste und wählen Sie den Befehl **SurfControl, Webseitenfilter aussetzen.** Sie können auch beim Microsoft Internet Explorer auf die SurfControl Schaltfläche gehen und den Webseitenfilter mit der linken Maustaste aussetzen. Beachten Sie, dass Sie bei aktivierter SurfControl ein Passwort eingeben müssen, um sie zu deaktivieren.

Option	Beschreibung
Webseitenfilter	**Normale Filterfunktion** oder **Nur protokollieren.** Ändern Sie den Modus für den Webseitenfilter, und legen Sie fest, wie unerwünschte Webseiten analysiert und blockiert werden sollen. Klicken Sie auf **Konfigurieren,** um den aktuellen Modus des Webseitenfilters zu ändern. Die Standardeinstellung ist **Normale Filterfunktion. Nur protokollieren** blockt keine unerwünschten Inhalte, sondern zeichnet diese Zugriffe lediglich auf.
Anwendungs-steuerung	**Passwort erforderlich** oder **Kein Passwort.** Wenn die Anwendungssteuerung aktiviert ist, benötigen Anwendungen eine Zugriffsberechtigung, wenn sie zum ersten Mal eine Verbindung zum Internet aufbauen. Bei aktivierter SurfControl ist zur Vergabe dieser Berechtigung ebenfalls die Eingabe des Passworts erforderlich.
Zugelassene/ gesperrte Webseiten	Zeigt die Anzahl der Webseiten an, die gegenwärtig zugelassen oder gesperrt sind. Klicken Sie auf **Ansicht ...,** um die Webseiten-Liste anzuzeigen. Dort können Sie die zugelassenen und gesperrten Webseiten konfigurieren sowie sich das Protokoll aller aufgerufenen Webseiten ansehen.
Erweitert ...	Öffnet die Registerkarte SurfControl im Fenster **Erweiterte Einstellungen** für weitere Konfigurationen der SurfControl.

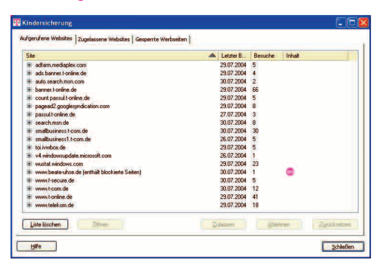
7.1 Webseitenfilter

Der Webseitenfilter bestimmt, welche Webseiten gefiltert werden. Sie können die Filterstufe für Webseiten ändern, um festzulegen, ob Sie die normale Filterfunktion aktivieren, alle besuchten Webseiten protokollieren oder den Webseitenfilter vollständig deaktivieren möchten. Der Webseitenfilter filtert nur HTTP-Webseiten nach den ausgewählten Kategorien.

Hinweis: HTTPS-Seiten können nicht gefiltert werden, weil sie verschlüsselt sind.

Wichtig: Keine Blockierungssoftware ist beim Filtern aller unerwünschten Webseiten 100%ig erfolgreich. Sie können unerwünschte Webseiten zur Liste der gesperrten Webseiten hinzufügen, wenn kein Zugriff auf diese Seiten möglich sein soll.

7.2 Aufgerufene Webseiten



In der Liste **Aufgerufene Webseiten** werden alle protokollierten Webseiten aufgeführt, auf die Sie zugegriffen haben. Webseiten werden in der Liste **Aufgerufene Webseiten** nur dann protokolliert, wenn als Modus für den Webseitenfilter **Normale Filterfunktion** oder **Nur protokollieren** ausgewählt wurde. In der Liste **Gesperrte Webseiten** werden alle besuchten Webseiten aufgeführt. In der Liste werden Webseiten farbcodiert:

Rot Die Webseite befindet sich in der Liste der gesperrten Webseiten.
Grün Die Webseite befindet sich in der Liste der zugelassenen Webseiten.
Blau Die Webseite enthält eine oder mehrere zugelassene oder abgelehnte Seiten, die vom Webseitenfilter blockiert wurden.

Das Inhaltssymbol zeigt den Grund an, aus dem der Filter der SurfControl die Webseite blockiert hat:

 Drogen  Hass Glücksspiel  Sex  Waffen  Webmail

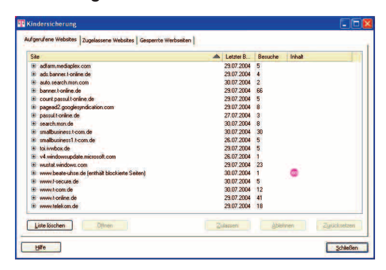
- Klicken Sie auf den Button **Liste löschen,** um alle Webseiten aus der Liste der aufgerufenen Webseiten zu löschen. Wenn Sie den Inhalt der Liste der aufgerufenen Webseiten löschen, wirkt sich das nicht auf die Listen der zugelassenen und gesperrten Webseiten aus.
- Klicken Sie auf **Öffnen,** um die ausgewählte Webseite im Standard-Webbrowser zu öffnen.
- Klicken Sie auf **Löschen,** um den gewünschten Eintrag aus der Liste zu entfernen.

- Klicken Sie auf **Zulassen,** um Webseiten zur Liste der zugelassenen Webseiten hinzuzufügen.
- Klicken Sie auf **Ablehnen,** um Webseiten zur Liste der gesperrten Webseiten hinzuzufügen.

7.3 Zugelassene und gesperrte Webseiten

Der Webseitenfilter analysiert und filtert Webseiten automatisch anhand ihrer Inhalte. Wenn Sie blockierte Webseiten zulassen oder weitere Webseiten sperren möchten, können Sie diese Einstellungen in den Listen der zugelassenen und gesperrten Webseiten durchführen.

7.3.1 Zugelassene Webseiten

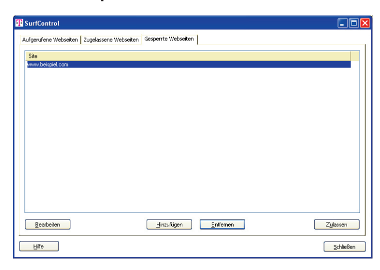


Die Liste der zugelassenen Webseiten enthält alle Webseiten, die aufgerufen werden können, selbst wenn die Webseite sonst von der SurfControl gefiltert würde. Wenn Sie zugelassene Seiten aufrufen, fordert Sie die SurfControl nicht zur Eingabe des Passworts auf.

- Klicken Sie auf **Hinzufügen ...,** um eine neue Webseite zur Liste der zugelassenen Webseiten hinzuzufügen.
- Wenn Sie alle Seiten einer kompletten Seite, z. B. www.beispiel.com, zulassen möchten, geben Sie beispiel.com in das Adressfeld ein. Wenn Sie nur einen Teil der Webseite www.beispiel.com zulassen möchten, geben Sie beispiel.com/unterseite ein.
- Klicken Sie auf **Bearbeiten ...,** um die Einstellungen für die ausgewählte Webseite zu bearbeiten.
- Klicken Sie auf **Entfernen,** um die ausgewählte Webseite aus der Liste zu entfernen.
- Klicken Sie auf **Ablehnen,** um die zugelassene Webseite in die Liste der gesperrten Webseiten zu verschieben.

Hinweis: Sie können außerdem im Internet Explorer eine neue zugelassene Webseite über die Menüschaltfläche **Webfilter** von **SurfControl** hinzufügen. Wählen Sie mit der linken Maustaste **Diese Webseite zulassen ...,** um die aktuelle Seite zur Liste der zugelassenen Webseiten hinzuzufügen.

7.3.2 Gesperrte Webseiten



Die Liste der gesperrten Webseiten enthält alle Webseiten, auf die ein Zugriff ohne Eingabe eines Passworts nicht möglich ist.

- Klicken Sie auf **Hinzufügen ...,** um eine neue Webseite zur Liste der gesperrten Webseiten hinzuzufügen.
- Wenn Sie alle Seiten einer kompletten Seite, z. B. www.beispiel.com, sperren möchten, geben Sie www.beispiel.com in das Adressfeld ein. Wenn Sie nur einen Teil der Webseite www.beispiel.com sperren möchten, geben Sie www.beispiel.com/unterseite ein.
- Klicken Sie auf **Bearbeiten ...,** um die Einstellungen für die ausgewählte Webseite zu bearbeiten.
- Klicken Sie auf **Entfernen,** um die ausgewählte Webseite aus der Liste zu entfernen.
- Klicken Sie auf **Zulassen ...,** um eine gesperrte Webseite in die Liste der zugelassenen Webseiten zu verschieben.

Hinweis: Sie können außerdem im Internet Explorer eine neue abzulehnende Webseite über die Menüschaltfläche **Webfilter** von **SurfControl** hinzufügen. Wählen Sie mit der linken Maustaste **Diese Webseite sperren ...,** um die aktuelle Seite zur Liste der gesperrten Webseiten hinzuzufügen.

7.4 Passwort für SurfControl

Das Passwort für SurfControl schützt die Programmkonfiguration vor Änderungen. Sie müssen das Passwort eingeben, wenn Sie die folgenden Vorgänge ausführen möchten:

- Programm starten und Einstellungen konfigurieren
- Webseitenfilter vorübergehend aussetzen
- Liste der Webseiten anzeigen
- Alarmmeldungen des Internet-Schutzschilds anzeigen
- Gesamten Datenverkehr zulassen
- Programme aus dem Speicher entfernen
- Anwendungen den Zugriff auf das Internet erlauben
- Deinstallation der Software (falls erwünscht)

Sie erstellen das Passwort während der Installation. Sie können das aktuelle Passwort über die erweiterten Funktionen der SurfControl ändern. Sie müssen Ihr aktuelles Passwort eingeben, bevor Sie ein neues festlegen können. Wenn Sie Ihr Passwort vergessen haben, können Sie es durch die Eingabe Ihres Registrierungsschlüssels zurücksetzen.

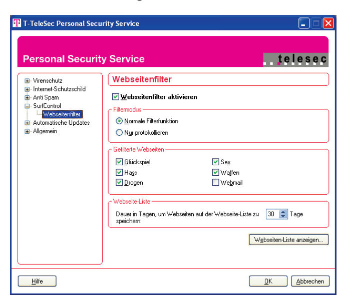


Wichtig: Sie sollten Ihren Registrierungsschlüssel geheim halten, damit nur Sie das Passwort ändern können.

7.4.1 Erstellen des Passworts für SurfControl

Wenn Sie Ihr Passwort erstellen, sollten Sie die folgenden Hinweise beachten:

- Verwenden Sie ein Passwort, das leicht zu merken, aber schwer zu erraten ist.
- Das Passwort kann aus beliebigen Zeichen zusammengesetzt und bis zu 80 Zeichen lang sein.



Auf der Seite mit den **erweiterten Einstellungen von SurfControl** können Sie den Status des Webseitenfilters und des Passwort-Cache-Speichers anzeigen. Sie können außerdem Ihr aktuelles Passwort ändern und den Passwortschutz zu neuen Verbindungen und der Programmdeinstallation hinzufügen.

Option	Beschreibung
Webseitenfilter	**Aktiviert, Deaktiviert** oder **Vorübergehend angehalten.** Klicken Sie auf **Aktivieren** oder **Deaktivieren,** um den aktuellen Modus des Webseitenfilters zu ändern.
Dialogfeld zur Anwendungssteuerung anzeigen und Passwort abfragen	Wenn Sie als Einstellung **Aktiviert** auswählen, können Anwendungen, die Sie nicht ausdrücklich zugelassen haben, ohne Ihre Autorisierung keine Verbindung mit dem Internet aufbauen. Sie können Anwendungen mittels Eingabe des Passworts zulassen. Sie können diese Einstellung nicht auswählen, wenn der Internet-Schutzschild nicht installiert ist.
Deinstallation nur mit Passwort	Wenn diese Einstellung aktiviert ist, können Benutzer nur mit der Eingabe des Passworts das Programm deinstallieren.

Option	Beschreibung
Keine Passwortabfrage für [ ] Sekunden	Hiermit können Sie während eines bestimmten Zeitraums Aktionen ausführen, die normalerweise die Eingabe eines Passworts erfordern würden. Darüber hinaus können Sie bei jeder Eingabe Ihres Passworts entscheiden, dieses für die Dauer der Sitzung im Speicher zu behalten. Auf diese Weise müssen Sie Ihr Passwort nicht erneut eingeben, bevor Sie sich vom Computer abmelden.
Passwort ändern ...	Mit diesem Befehl ändern Sie Ihr aktuelles Passwort.

Webseitenfilter

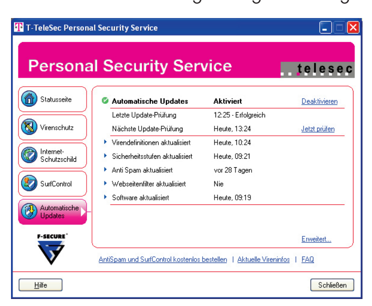
Auf der Seite **Webseitenfilter** legen Sie die Inhalte fest, die gefiltert werden sollen.

Option	Beschreibung
Webseitenfilter aktivieren	Schaltet den Webseitenfilter ein. Wenn Sie den Webseitenfilter deaktivieren, werden keine Webseiten blockiert oder protokolliert.
Filtermodus	**Normale Filterfunktion** oder **Nur protokollieren. Normale Filterfunktion** analysiert Webseiten und blockiert unerwünschte Seiten anhand ihrer Inhalte. Wenn als Filtermodus **Nur protokollieren** ausgewählt ist, werden keine Webseiten vom Webseitenfilter blockiert, jedoch werden alle aufgerufenen Webseiten auf der Webseiten-Liste der aufgerufenen Webseiten protokolliert.
Gefilterte Webseiten	Wählen Sie den Webseiteninhalt, der gefiltert werden soll. **Vorsicht:** Nach Auswahl der Kategorie Webmail können Sie keine Mails mehr über den Browser abrufen (z. B. GMX, web.de etc.).
Dauer in Tagen, um Webseiten auf der Webseiten-Liste zu speichern	Mit dieser Option legen Sie fest, wie lange protokollierte Webseiten in der Webseiten-Liste gespeichert werden, bevor die Einträge automatisch gelöscht werden.
Webseiten-Liste anzeigen	Öffnet die Webseiten-Liste für SurfControl. Sie können sich dort alle aufgerufenen Webseiten ansehen und dort auch zugelassene sowie gesperrte Webseiten hinzufügen und konfigurieren.

8. Automatische Updates



Der automatische Aktualisierungsdienst wird transparent im Hintergrund aktiviert. Wenn Sie eine Verbindung zum Internet herstellen, wird gewährleistet, dass Sie die aktuellsten Updates auf Ihren Computer erhalten. Sie können im Bereich der automatischen Aktualisierungen folgende Vorgänge ausführen:



Option	Beschreibung
Automatische Updates	Zeigt den Status der automatischen Updates an. Klicken Sie auf **Aktivieren** bzw. auf **Deaktivieren,** um **Automatische Updates** zu aktivieren oder zu deaktivieren.
Letzte Update-Prüfung	Zeigt die Uhrzeit und den Status des letzten Updates an.
Nächste Update-Prüfung	Zeigt die Uhrzeit und den Status des nächsten Updates an. Wenn Sie selbst prüfen möchten, ob Sie über die aktuellen Virendefinitionen verfügen, klicken Sie auf **Jetzt prüfen.** Wenn Ihre Definitionen nicht auf dem neuesten Stand sind, werden die aktuellen Versionen heruntergeladen.
Virusdefinitionen aktualisiert	Zeigt die Uhrzeit der letzten Aktualisierung der Virendefinitionen an.
Sicherheitsstufen aktualisiert	Zeigt das Datum der letzten Aktualisierung der Sicherheitsstufen an.
Anti Spam aktualisiert	Zeigt das Datum der letzten Aktualisierung von Anti Spam an.

Option	Beschreibung
Webseitenfilter aktualisiert	Zeigt das Datum der letzten Aktualisierung des Webseiten-filters an.
Software aktualisiert	Zeigt das Datum der letzten Produktaktualisierung an.
Erweitert	Öffnet die Registerkarte **Automatische Updates** im Fenster **Erweiterte Einstellungen.**

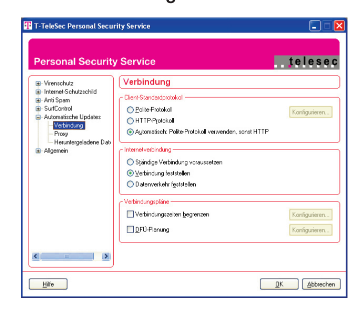
Hinweis: Über das Kontrollkästchen **Erinnerung** können Sie auswählen, nach wie vielen Tagen Sie an ein neues Update erinnert werden möchten.

Hinweis: Wenn Sie ein Modem verwenden bzw. über eine ISDN-Verbindung zum Internet verfügen, muss die Verbindung aktiv sein, damit geprüft werden kann, ob Updates vorliegen.

ISDN: Automatische Updates sind standardmäßig einmal pro Stunde eingeplant. Das bedeutet, dass einmal pro Stunde eine Internetverbindung hergestellt wird, wenn Sie über einen ISDN-Router bzw. ein automatisches Wählgerät verfügen (jede Verbindung ist gebührenpflichtig). Wenn Sie die automatische Wahlfunktion Ihres ISDN-Routers ausschalten möchten, deaktivieren Sie die automatischen Updates, und klicken Sie auf die Schaltfläche **Jetzt prüfen,** um festzustellen, ob neue Updates verfügbar sind, oder die geplanten Verbindungszeiten einzuschränken.

8.1 Erweiterte Einstellung

8.1.1 Verbindung

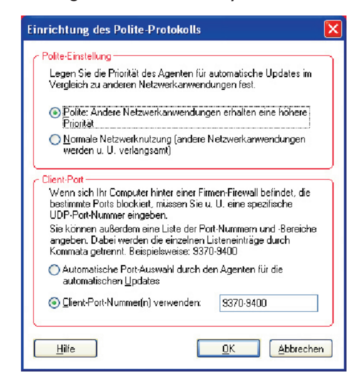


8.1.1.1 Client-Standardprotokoll

Wenn Sie mit dem Agenten für automatische Updates Virendefinitionen erhalten, können Sie nach der Installation die Methode auswählen, mit der eine Verbindung zum Update-Server aufgebaut wird. Voreingestellt und empfehlenswert ist: **Automatisch: Polite-Protokoll verwenden, sonst HTTP,** da die Anwendung je nach Auslastung automatisch auf das andere Protokoll wechselt, um die Verbindung zu verbessern.

Zur Auswahl stehen **Polite-Protokoll** oder **HTTP-Protokoll.** Wenn Sie sich für das Polite-Protokoll entscheiden, klicken Sie auf die Schaltfläche **Konfigurieren** neben dieser Methode, um die Einstellungen für das Polite-Protokoll anzupassen. Weitere Informationen zu den Einstellungen finden Sie im Abschnitt 8.1.1.2 Einrichtung des Polite-Protokolls auf Seite 103. Falls Probleme mit dem Polite-Protokoll auftreten, können Sie auch **Automatisch: Polite-Protokoll verwenden, sonst HTTP** auswählen. Bei Aktivierung dieser Option wird HTTP für die Verbindung verwendet, wenn ein Verbindungsaufbau mit dem Polite-Protokoll nicht möglich war.

8.1.1.2 Einrichtung des Polite-Protokolls (können Sie über den Button Konfigurieren ... öffnen)



Mit den Optionen im Fenster **Einrichtung des Polite-Protokolls** können Sie die Priorität des Polite-Protokolls gegenüber anderen Netzwerkanwendungen festlegen.

Polite-Einstellung

- **Bei Auswahl der Option Polite:** Andere Netzwerkanwendungen erhalten eine höhere Priorität. Hierbei verwendet der automatische Update-Agent weniger Bandbreite, wenn auch andere Anwendungen Daten über das Netzwerk austauschen.
- **Bei Auswahl der Option Normale Netzwerknutzung** verwendet der Agent für automatische Updates so viel Bandbreite wie möglich, um die Virendefinitions-Updates herunterzuladen. Möglicherweise verlangsamen sich durch diese Option andere Netzwerkanwendungen.

Client-Port

Wenn sich Ihr Computer hinter einer Unternehmens-Firewall befindet, werden die vom Polite-Protokoll genutzten Ports unter Umständen blockiert. Das Polite-Protokoll verwendet zum Zugriff auf den Update-Server das UDP-Protokoll. Ist der entsprechende UDP-Port blockiert, kann keine Verbindung aufgebaut werden.

- Befindet sich Ihr Computer nicht hinter einer Unternehmens-Firewall, können Sie das Kontrollkästchen **Automatische Port-Auswahl durch den Agenten** für die automatischen Updates aktivieren.
- Wenn sich Ihr Computer hinter einer Unternehmens-Firewall befindet, fragen Sie bei Ihrem Netzwerkadministrator nach, welche Ports verwendet werden können. Geben Sie anschließend den oder die Ports in das Feld Client-Port-Nummer(n) verwenden: ein. Sie können eine durch Kommata getrennte Liste mit Port-Nummern und Port-Bereichen eingeben.

8.1.1.3 Unterschied Polite-Protokoll und HTTP

Der Vorteil des Polite-Protokolls ist der, dass Sie neben dem Update weiterhin im Internet surfen und Anwendungen des Internets nutzen können. Bei der Verwendung von HTTP wird eine größere Bandbreite der Internetverbindung für das Update genutzt und parallele Aktivitäten im Internet sind nur noch schwer möglich.

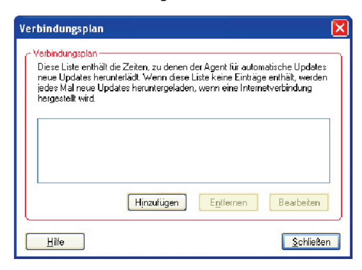
8.1.1.4 Internetverbindung

Es gibt drei Optionen, um festzustellen, ob zum Zeitpunkt des Verbindungsversuchs eine Internetverbindung verfügbar ist:

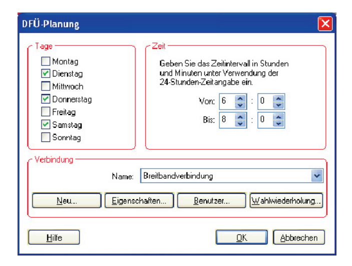
- **Ständige Verbindung voraussetzen –** Die automatische Update-Funktion setzt immer voraus, dass eine aktive Netzwerkverbindung vorhanden ist.
  Hinweis: Wenn Ihr Computer nicht über eine ständige Netzwerkverbindung verfügt und stattdessen ein DFÜ-Zugang eingerichtet wurde, kann diese Einstellung für wiederholte DFÜ-Einwahlversuche durch das Modul für die automatischen Updates verantwortlich sein.
- **Verbindung feststellen –** Diese Standard-Verbindung ist nach der Installation voreingestellt. Die automatische Update-Funktion erkennt, ob eine Netzwerkverbindung aktiv ist. Daten werden nur heruntergeladen, wenn eine aktive Verbindung gefunden wird.
- **Datenverkehr feststellen –** Die automatische Update-Funktion erkennt, ob eine Netzwerkverbindung aktiv ist, indem überprüft wird, ob andere Anwendungen auf das Netzwerk zugreifen. Diese Einstellung wird für Computer ohne ständige Verbindung zum Netzwerk empfohlen, bei denen auf Grund einer speziellen Hardwarekonfiguration immer eine Netzwerkverbindung festgestellt wird.

8.1.1.5 Verbindungspläne

Wenn Updates immer dann heruntergeladen werden sollen, wenn eine Internetverbindung verfügbar ist, achten Sie darauf, dass das Kontrollkästchen **Verbindungszeiten begrenzen** nicht aktiviert ist. Sie können einschränken, zu welchen Zeiten Updates heruntergeladen werden können. Aktivieren Sie dazu das Kontrollkästchen, und klicken Sie auf **Konfigurieren.** Daraufhin wird eine Liste mit Zeiträumen geöffnet, die Sie konfiguriert haben.



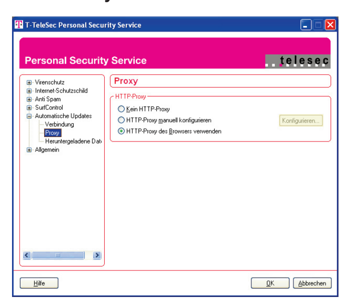
Wenn diese Liste keine Einträge enthält, werden jedes Mal neue Updates heruntergeladen, wenn eine Internetverbindung hergestellt wird. Wenn Sie einen Zeitraum zum Herunterladen von Updates hinzufügen möchten, klicken Sie auf **Hinzufügen.** Wählen Sie die Wochentage und Uhrzeiten, an denen Updates heruntergeladen werden können, und klicken Sie auf **OK.** Sie können auch mehrere Zeiträume hinzufügen, die alle in der Liste angezeigt werden. Wenn Sie eine DFÜ-Verbindung verwenden, können Sie die Verbindungszeiten mit Hilfe der DFÜ-Planung einschränken.



1. Aktivieren Sie das Kontrollkästchen **DFÜ-Planung.**
2. Klicken Sie auf **Konfigurieren,** um einen Zeitraum hinzuzufügen, in dem das Produkt eine Verbindung zum Internet aufbauen und neue Updates herunterladen kann.
3. Wählen Sie die Wochentage und Uhrzeiten, an denen Updates heruntergeladen werden sollen.

4. Wählen Sie die gewünschte DFÜ-Verbindung, oder klicken Sie auf **Neu ...,** um eine neue Verbindung sowie einen neuen Verbindungstyp zu definieren. Klicken Sie auf **Eigenschaften ...** und **Benutzer,** um die Eigenschaften der DFÜ-Verbindung anzuzeigen und zu bearbeiten. Sie können die Häufigkeit der Wahlwiederholung anpassen, wenn die DFÜ-Verbindung nicht erfolgreich ist. Klicken Sie dazu auf **Wahlwiederholung ...**
5. Klicken Sie auf **OK,** um die Bearbeitung der DFÜ-Planung abzuschließen.

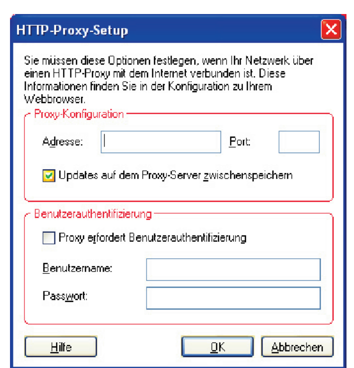
8.1.2 Proxy



Im Abschnitt **Proxy** können Sie die Proxy-Einstellungen für die automatische Update-Funktion einrichten, wenn der Datenverkehr über einen Proxy-Server geleitet wird. Sie können folgende Optionen auswählen:

- **Kein HTTP-Proxy** bei Nutzung einer direkten Verbindung.
- **HTTP-Proxy manuell konfigurieren,** wenn Sie die Proxy-Einstellungen speziell für einen Proxy-Server eingeben möchten. Klicken Sie auf die Schaltfläche **Konfigurieren,** um das Dialogfeld HTTP-Proxy-Setup zu öffnen.
- **HTTP-Proxy des Browsers verwenden,** wenn Sie mit denselben Proxy-Einstellungen arbeiten möchten, die bereits für Ihren Standard-Browser festgelegt wurden.

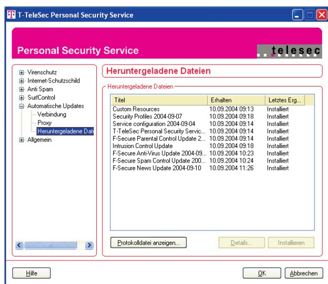
8.1.2.1 HTTP-Proxy-Setup (über den Button Konfigurieren zu öffnen)



Geben Sie in das Dialogfeld **HTTP-Proxy-Setup** die Einstellungen für Ihren Proxy-Server ein. Geben Sie zunächst die IP-Adresse und die Port-Nummer des Proxy-Servers in die Felder **Adresse** und **Port** ein.

- Wenn das Update nach dem Herunterladen weiterhin im Proxy-Cache gespeichert bleiben soll, aktivieren Sie das Kontrollkästchen **Updates auf dem Proxy-Server zwischenspeichern.** Andere Benutzer können das Update dann direkt vom Proxy herunterladen. Der Proxy muss in diesem Fall die Daten nicht erneut vom Server herunterladen.
- Wenn für den Zugriff auf den Proxy-Server eine Benutzerauthentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **Proxy erfordert Benutzerauthentifizierung,** und geben Sie Ihren Benutzernamen und Ihr Passwort in die Felder Benutzername und Passwort ein.

8.1.3 Heruntergeladene Dateien



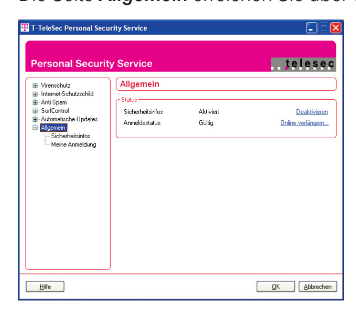
In der Liste Heruntergeladene Dateien werden alle heruntergeladenen Softwarepakete mit dem Zeitpunkt ihres Empfangs aufgeführt. Außerdem ist angegeben, ob die Pakete installiert wurden.

- Klicken Sie auf **Protokolldatei anzeigen,** um das Protokoll der Download-Informationen anzuzeigen.
- Klicken Sie auf **Details ...,** um weitere Informationen (Name des Pakets, Datum des Downloads, Größe der Datei und ob die Installation erfolgreich war) zum ausgewählten Softwarepaket anzuzeigen.
- Klicken Sie auf **Installieren,** um das ausgewählte Softwarepaket zu installieren, falls das noch nicht geschehen ist.

9. Allgemein

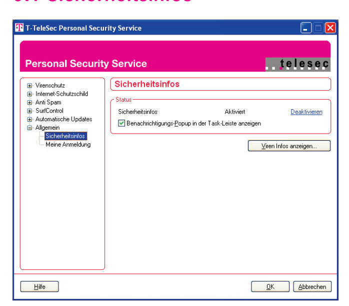


Die Seite **Allgemein** erreichen Sie über die **Erweiterten Einstellungen** im Hauptmenü.



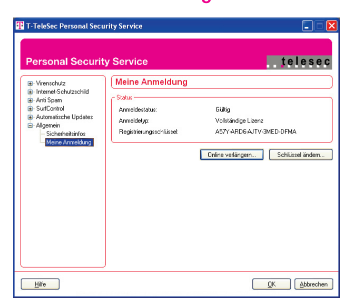
Sicherheitsinfos – Zeigt den Status der Sicherheitsinfos an. Klicken Sie auf **Aktivieren** bzw. auf **Deaktivieren,** um die Sicherheitsinfos zu aktivieren oder zu deaktivieren.
Meine Anmeldung – zeigt an, ob Sie im Besitz eines gültigen Registrierungs-schlüssels sind.

9.1 Sicherheitsinfos



Über dieses Statusfenster können Sie zum einen die Sicherheitsinfos aktivieren und deaktivieren und zum anderen können Sie, indem Sie die Checkbox **Benachrichti-gungs-Popup in der Task-Leiste anzeigen** anklicken, entscheiden, ob Sie einen zusätzlichen Hinweis bei einer neuen Virenwarnung neben der Uhranzeige haben möchten. Wenn Sie den Button **Viren Infos anzeigen** anklicken, werden Ihnen alle aktuellen Viren-Infos angezeigt.

9.2 Meine Anmeldung



Die Seite Meine Anmeldung zeigt Informationen zur eigenen Anmeldung an.

Auf der Seite Meine Anmeldung stehen Ihnen folgende Optionen zur Verfügung:

- Anzeigen des Anmeldestatus
- Anmeldetyp
- Registrierungsschlüssel

Über den Button **Online verlängern ...** können Sie einen neuen Registrierungsschlüssel bestellen, falls Ihrer abgelaufen ist oder Sie einen zweiten Registrierungsschlüssel für einen weiteren PC erwerben möchten.
Über den Button **Schlüssel ändern ...** können Sie den alten Registrierungsschlüssel per Copy and Paste gegen einen neuen Schlüssel bei bestehender Internetverbindung austauschen.

Hinweise: Angenommen, Sie hatten zuvor eine 30-Tage-Testversion und möchten nun den vollwertigen Registrierungsschlüssel verwenden. In dem Fall müssen Sie nicht die Software deinstallieren und mit einem neuen Schlüssel neu installieren. Mit **Schlüssel ändern ...** wird der Austausch vereinfacht. Wenn Sie Windows NT 4.0, Windows 2000 oder Windows XP verwenden und über mehr als ein Benutzerkonto verfügen, müssen Sie sich als Administrator anmelden, um für Personal Security Service Ihren Registrierungsschlüssel zu ändern.

10. So schützt Personal Security Service Ihren Computer

10.1 Virenschutz

Programme oder Dateien wie beispielsweise Viren, Würmer, Trojanische Pferde, Jokes und Fehlermeldungen, die entwickelt werden, um auf Ihrem Computer Schaden anzurichten, werden als Malware (abgeleitet von „malicious software") bezeichnet. Der Virenschutz entdeckt und entfernt (desinfiziert) Viren und andere bösartige Computerprogramme von Ihrem Computer. Der Virenschutz von Personal Security Service prüft Dateien bei jedem Öffnen von der Festplatte, einem externen Speichermedium oder dem Internet auf Viren. Ab der Version 5.0 werden Viren, Würmer und Trojaner schon direkt beim Download von E-Mails entdeckt, bevor Sie auf Ihrem Computer abgespeichert werden. Aktuellste Virenschutzsoftware und automatisch aktualisierte Virendefinitionen bieten Ihnen den besten Schutz gegen Viren. Das Forschungslabor von F-Secure Anti-Virus veröffentlicht und aktualisiert regelmäßig Virendefinitionen, Profile und die Personal Security Service Software, die bei jeder Verbindung mit dem Internet schnell und automatisch von Personal Security Service heruntergeladen werden. Der Virenschutz von Personal Security Service verwendet mehrere Virusscanmodule, um lückenlosen Schutz gegen Viren zu gewährleisten. Von diesen schützt besonders das Modul für heuristisches Scannen gegen neue und unbekannte Viren.

10.2 Internet-Schutzschild

Bei jeder Verbindung, die Ihr Computer zum Internet herstellt, ist er ein mögliches Ziel für Internet-Angriffe aus unbekannten Quellen. In einigen Fällen sind dies jedoch keine wirklichen Angriffe, sondern harmlose Meldungen, die versehentlich bei Ihrem Computer eingehen. Es kann in anderen Fällen allerdings auch vorkommen, dass ein unbekannter Dritter oder ein Computer vorsätzlich versucht, auf Ihren Computer und Ihre Dateien zuzugreifen. Des Weiteren gibt es auch arglistige Programme, auch Dialer genannt, die Sie sich unbeabsichtigt und ungewollt auf Ihren PC herunterladen. Ohne Ihre Kenntnisnahme verbinden sich diese Programme via DFÜ, TAPI oder CAPI zu einer kostenpflichtigen Rufnummer (z. B. 0190/0900). Der Internet-Schutzschild

erkennt ALLE Wählversuche, die über die Windows-DFÜ-Steuerung, TAPI oder CAPI erfolgen, und fordert Sie anschließend auf, sich zu entscheiden, ob die Verbindung zugelassen oder abgelehnt werden soll. Sicherheitslücken für Ihren Computer ergeben sich auf vielfache Weise, wie beispielsweise durch Folgendes:

- Versehentlich offen gelassene Dienstprogramme können von Dritten problemlos gefunden und missbraucht werden.

Der Internet-Schutzschild schützt Ihren Computer bei Verbindungen zum Internet. Er lässt nur die Verbindungen für Ihren Computer zu, die im ausgewählten Profil zugelassen sind. Datenverkehr über andere als diese Verbindungen wird verhindert, so dass Hacker nahezu keine Chance haben, die Informationen auf Ihrem Computer einzusehen oder zu manipulieren.

- Ihr Computer überträgt Informationen über sein System. Wenn Sie eine Internetverbindung hergestellt haben, kann jeder, der sich damit auskennt, diese Informationen als Grundlage für einen Angriff gegen Sie verwenden. Der Internet-Schutzschild verhindert, dass Ihr Computer im Internet Systeminformationen sendet, und sorgt dafür, dass keine Informationen über Sie oder Ihren Computer über ausgehende Verbindungen freigegeben werden.
- Einige Trojanische Pferde verstecken sich in Software, der Sie normalerweise vertrauen. Sie nutzen eine Verbindung oder Anwendung, die Sie für sicher halten, um Daten über Sie oder Ihren Computer zu übertragen. Der Internet-Schutzschild erkennt Datenübertragungsversuche von Trojanischen Pferden und verhindert das Herstellen der Verbindung, so dass Ihre Daten jederzeit gegen unerwünschte Angriffe geschützt sind.
- Das neue Leistungsmerkmal ab der Version 5.0, Intrusion Prevention, stellt einen zusätzlichen Schutz zu der bereits vorhandenen Firewall dar. Die Firewall legt in aller Regel Dienst, Port und Richtung der zugelassenen Internetverbindungen fest. Intrusion Prevention analysiert den gesamten Datenverkehr, um diesen nach Angriffsmustern zu untersuchen. Dazu gehören beispielsweise Port-Scans und

Angriffe auf Ports, die von der Firewall nur ausgehend geöffnet sind. Diese werden häufig mit manipulierten Datenpaketen, die sich als Antwortpakete auf Aktionen des Hosts ausgeben, durchgeführt. Derartige Angriffe werden von Intrusion Prevention erkannt und geblockt.

10.3 Anti Spam

Das große Problem der Spam-E-Mails ist die Abwälzung der Kosten auf die Empfänger und die Provider. Das SMTP-Protokoll, das technisch den Versand von E-Mails regelt, ermöglicht es, zu einer E-Mail eine Liste von 100 Empfängern anzugeben, an die der Mailserver die E-Mail verschickt. Wenn der Spammer also eine Million E-Mails versenden will, muss er lediglich 10.000 Mal eine E-Mail verschicken. Die ganze restliche Last tragen die Provider und die Empfänger. Allein die Kosten des Downloads von Spam-Mails bei den Empfängern werden auf weltweit jährlich 10 Mrd. € geschätzt.
Ein anderes Problem sind die durch den Spam-Versand entstehenden Verzögerungen und Ausfälle. Alle auf dem Mailserver zum Versand anstehenden Mails landen in einer Warteschleife. Wenn ein Spammer nun 1.000.000 Spams in die Warteschleife setzt, müssen auch normale Mails hinten anstehen und werden so erst mit erheblicher Verzögerung weiterverschickt. Viele Mailboxen haben auch heute noch eine Größenbeschränkung. Oft passiert es, dass z. B. bei Ferienabwesenheit so viele Spams eintreffen, dass die Mailbox überfüllt ist und reguläre Mails abgewiesen werden. Durch übermäßige Nutzung können Server sogar abstürzen, was massive Verzögerungen und gravierende Schäden zur Folge haben kann.
Spams sind somit ein Ärgernis für alle E-Mail-Benutzer. Sie machen viele Dienstleistungen unmöglich oder erschweren sie gravierend. Mailinglisten können vielfach nur mit einem Moderator geführt werden, der Spam-Mails vorrangig löscht. Viele Personen geben auch ihre Mailadresse nicht mehr an, aus Angst, zugespammt zu werden. Dies erschwert die Kommunikation oder macht sie unmöglich.

Um Spam-E-Mails zu verhindern, bietet Personal Security Service die folgenden Funktionen: Sämtliche eingehenden E-Mails werden während der Übermittlung auf den Benutzer-Computer auf Spam-E-Mails hin überprüft. Der Spam-Filter kennzeichnet alle E-Mails, bei denen es sich um Spam-E-Mails handelt in der Betreff-Zeile. Der

Spam-Filter arbeitet wie ein POP3-Proxy-Server, der zwischen dem E-Mail- und dem Mail-Server platziert ist.

- **Analyse des E-Mail-Headers und des E-Mail-Inhalts**
  Drei vordefinierte Filter Profile – Es stehen drei vordefinierte Filter Profile zur Auswahl. Somit können Sie (auch ohne Computer-Fachkenntnisse), die entsprechende Einstellung Ihren Bedürfnissen entsprechend vornehmen. Die Profile lassen sich einfach mit einem Mausklick auswählen.
- **Kategorisierung der eingehenden E-Mails**
  E-Mails von Absendern, die als Spam-Mails definiert sind, werden beim Eingehen direkt in den Spam-Ordner verschoben.
- **Listen Gefilterte Absender und Zugelassene Absender**
  Sie haben die Möglichkeit, eigene Listen der zuzulassenden und abzulehnenden E-Mail-Adressen und/oder Domänen zu erstellen. Dadurch werden die Präzision der Filterung sowie die Filter-Geschwindigkeit erhöht. Die Listen können im E-Mail-Client (Outlook und Outlook Express) gepflegt werden.
- **Automatische Aktualisierung**
  Die Aktualisierung des Spam-Filter-Moduls erfolgt wie bisher via automatisches Update, ohne dass Sie sich darum kümmern müssen.
- **Eigene Domäne und persönliche Kontakte**
  Sie können vertrauenswürdige E-Mail-Adressen (eigene Domäne, persönliche Kontakte aus dem Adressbuch) als zugelassene Absender definieren. Die E-Mails dieser Absenderadressen werden nicht auf Spam hin überprüft.
- **Integrierter Virenschutz**
  Sämtliche eingehenden und ausgehenden E-Mails werden auf Viren überprüft.

10.4 SurfControl

Das Software-Paket SurfControl sorgt nicht nur für eine „digitale Kindersicherung“, die es ermöglicht, bestimmte Internetseiten für Kinder zu sperren. Die Software dient ebenso Firmenchefs, die das Surfverhalten Ihrer Mitarbeiter einschränken und überprüfen möchten. Mit SurfControl ist es beispielsweise möglich, Internetseiten mit pornografischen oder kriminellen Inhalten für Kinder anhand der Auswahl von Kategorien unzugänglich zu machen. Das Programm beinhaltet typische Filterkategorien, die

vom Administrator als **Zugelassen** oder **Abgelehnt** ausgewählt werden können. Eine freie Konfiguration, z. B. anhand von explizit abzulehnenden URLs, ist ebenfalls möglich. SurfControl ist einfach zu konfigurieren und bietet durch die ständigen automatischen Updates einen guten Schutz für Kinder und eine erhöhte Produktivität der Mitarbeiter.

- Einfache Nutzung
- Benutzerfreundliche Bedienung
- Browser-Plug-in
- Falls der Zugriff auf spezifische URLs nicht gestattet ist und Sie auf diese zugreifen, wird der Grund des verbotenen Zugriffs angezeigt.
- Sämtliche Einstellungen und Änderungen erfordern die Eingabe des Administratorpassworts.
- Administratorpasswort:
  Das Administratorpasswort wird direkt bei der Installation abgefragt. Einstellungen (z. B. Sperren von bestimmten URLs, Änderungen von Profilen etc.) können nur mit der Eingabe des Administratorpassworts durchgeführt werden. Deswegen müssen Sie das Passwort sicher aufbewahren.
- Filterkategorien:
  Es besteht die Option, die im Folgenden beschriebenen Kategorien zuzulassen oder abzulehnen:
  

  Hass Glücksspiel Sex Waffen
  

- Protokollierung:
  Hier wird jeder Versuch eines jeden Benutzers aufgezeichnet, eine URL aufzurufen, die nicht gestattet ist.
- Aktualisierung:
  Software- und Engine-Updates erfolgen auf dem gleichen Wege wie bisher mittels automatischem Update bei bestehender Internetverbindung.

10.5 So schützen Sie sich gegen Viren und andere Malware

Personal Security Service bietet den besten Schutz gegen Viren, da er bekannte Viren bereits unschädlich macht, bevor sie den Computer infizieren können. Zum Schutz Ihres Computers können Sie jedoch auch durch Folgendes beitragen:

- Halten Sie Ihr Betriebssystem und Ihre Anwendungen auf dem neuesten Stand, und wenden Sie aktuelle Patches an, sobald diese verfügbar sind. Beziehen Sie Aktualisierungen immer direkt vom Händler.
- Speichern Sie heruntergeladene Dateien immer zuerst auf Ihrer Festplatte, bevor Sie sie öffnen oder ausführen. Durch das Speichern von heruntergeladenen Dateien wird gewährleistet, dass Personal Security Service diese überprüft.
- Die meisten Würmer nutzen E-Mails zur Ausbreitung und sind auf Benutzer von Microsoft Outlook oder Outlook Express ausgerichtet. Wenn Sie eine Outlook-Version verwenden müssen, laden Sie sich regelmäßig den aktuellsten Sicherheitspatch für Microsoft Outlook herunter, und installieren Sie diesen auf Ihrem System.
- Wenn Sie E-Mail-Werbung oder unerwünschte E-Mails erhalten oder eine von einem Freund oder Bekannten erhaltene E-Mail merkwürdig scheint, öffnen Sie die Anhänge nicht bzw. klicken Sie nicht auf die enthaltenen Weblinks. Wenn Sie einen Anhang öffnen möchten, speichern Sie diesen auf Ihrer Festplatte, und öffnen Sie ihn von dort aus. Dadurch wird gewährleistet, dass Personal Security Service den Anhang auf Viren überprüft.
- Vermeiden Sie Dateien von öffentlichen Newsgroups und Online-Chat-Systemen wie beispielsweise IRC oder ICQ.
- Leiten Sie keine Virenwarnungen oder Kettenbriefe weiter, die Sie von anderen Absendern erhalten.

Häufig gestellte Fragen (FAQ)

PSS Betrieb allgemein

F: Personal Security Service ist sehr langsam bzw. kann nicht geöffnet werden. Wo liegt der Fehler?

A: Internet Explorer 5.0 oder höher ist unter Umständen nicht installiert. Überprüfen Sie, welche Version des Internet Explorers installiert ist (der Internet Explorer ist über die Webseite der Microsoft Corporation erhältlich: http://windowsupdate.microsoft.com

F: Das Taskleisten-Symbol wird nicht in der unteren rechten Ecke des Bildschirms neben der Uhr angezeigt.

A: Unter Windows XP können Symbole ausgeblendet werden. Um ausgeblendete Symbole anzuzeigen, klicken Sie auf die Schaltfläche «.
Bei NT-Betriebssystemen kann es durch eine Überlastung des PCs zu einem Absturz des Management-Agents kommen. Dies führt auch dazu, dass das Symbol nicht angezeigt wird. Dies können Sie beheben, indem Sie wie folgt vorgehen:

- Gehen Sie auf Start → Ausführen und geben Sie **cmd** ein.
- Drücken Sie **ENTER.**
- Geben Sie **net stop fsma** ein und drücken Sie **ENTER.**
- Warten Sie, bis der Management-Agent gestoppt wurde.
- Geben Sie **net start fsma** ein und drücken Sie **ENTER.**
- Warten Sie, bis der Management-Agent wieder gestartet ist.
- Geben Sie **exit** ein und drücken Sie **ENTER.**

Bei Misserfolg nach Ausführen der oben beschriebenen Schritte oder wenn Sie kein NT-Betriebssystem verwenden, ist das Programm nicht ordnungsgemäß installiert. Installieren Sie das Programm neu. Sollte eine Neuinstallation keinen Erfolg bringen, so wenden Sie sich an den Support.

F: Warum werden einige Einstellungen grau dargestellt, und warum kann ich diese nicht ändern?

A: Ihre Schutzstufe ist so eingestellt, dass Sie einige Einstellungen nicht ändern können. Wenn es möglich sein soll, dass Sie alle Einstellungen ändern können, wählen Sie eine benutzerdefinierte Schutzstufe.

F: Ich nutze Windows NT oder Windows 95. Warum bekomme ich nicht Anti Spam und/oder SurfControl?

A: Der Support für die beiden Betriebssysteme ist bei der neuen Version nicht mehr gegeben. Falls Sie diese Leistungsmerkmale nutzen wollen, ist ein Upgrade des Betriebssystems, z. B. auf Windows 2000 oder Windows XP, erforderlich.

F: Mein PC ist ein älteres Modell. Kann ich die Software trotzdem installieren?

A: Hierzu beachten Sie bitte die Mindestvoraussetzungen für den Betrieb der Software. Diese finden Sie im Handbuch. Bitte beachten Sie auch, dass diese Mindestanforderungen unter Umständen auch nicht ausreichend sind. Dies ist immer dann der Fall, wenn weitere Software auf dem PC installiert ist, die entweder im Hintergrund läuft, wie z. B. die Internetverbindungssoftware T-Online 5.0, oder gezielt genutzt wird, wie z. B. Bildbearbeitungsprogramme oder grafisch anspruchsvolle PC-Spiele. Bei einem gut genutzten System empfiehlt es sich, die Mindestanforderungen zu verdoppeln. Dadurch kann dann garantiert werden, dass die einzelnen Programme sich nicht gegenseitig ausbremsen und den PC langsam machen.

Installation

F: Das automatische Upgrade auf die neue Version hat nicht funktioniert. Was kann ich tun, um die neue Version zu erhalten?

A: Deinstallieren Sie die Software wie im Handbuch zu Personal Security Service beschrieben, laden Sie sich anschließend den aktuellen Software-Installer auf der Webseite www.t-com.de/pss herunter und installieren Sie diesen. Falls dann noch immer Probleme bestehen, wenden Sie sich bitte an den Support (siehe Abschnitt Technische Unterstützung auf Seite 130).

F: Sobald ich meinen Registrierungsschlüssel während der Installation eingegeben habe und dieser bei bestehender Internetverbindung verifiziert wurde, erhalte ich die Meldung, dass der Schlüssel abgelaufen ist, obwohl der Nutzungszeitraum noch nicht abgelaufen ist. Was kann ich tun?

A: Bitte wenden Sie sich an unseren Support (siehe Abschnitt Technische Unterstützung auf Seite 130). Bitte bedenken Sie, dass Sie einen Registrierungsschlüssel nur auf einem Computer zur gleichen Zeit verwenden können. Der Registrierungsschlüssel ist immer auf dem Computer verwendbar, auf dem die Software zuletzt installiert wurde. Voraussetzung hierfür ist eine vorherige komplette Deinstallation, wie im Handbuch beschrieben.

F: Der Registrierungsschlüssel kann nicht geprüft werden. Die Installation kann nicht weiter fortgeführt werden. Was ist geschehen?

A: Wenn keine Internetverbindung hergestellt wurde, konnte Personal Security Service Ihre Anmeldung nicht überprüfen. Prüfen Sie, ob eine Internetverbindung vorhanden ist, und installieren Sie Personal Security Service erneut.

F: Die Installation ist fehlgeschlagen. Nach der Installation bootet der PC nicht mehr ordnungsgemäß. Was ist nicht in Ordnung?

A: Sie haben vor der Installation von Personal Security Service evtl. vorhandene Antiviren- und Firewall-Programme von Drittanbietern nicht oder nur unvollständig deinstalliert. Was ist nun zu tun?
Starten Sie den PC im abgesicherten Modus. In den abgesicherten Modus kommen Sie bei den meisten Systemen, indem Sie direkt nach dem Einschalten die Taste **F8** drücken. Sollte Ihr BIOS eine andere Tastenbelegung vorgesehen haben, so schauen Sie bitte im Startmenü oder im Handbuch des BIOS nach. Im abgesicherten Modus deinstallieren Sie bitte zuerst PSS. Anschließend starten Sie den PC bitte neu, um die Ausgangssituation wiederherzustellen. Anschließend entfernen Sie bitte restlos alle Antiviren- und Firewall-Programme von Drittanbietern. Bitte achten Sie bei Windows XP darauf, dass die Verbindungsfirewall ausgeschaltet ist. Diese finden Sie in den TCP/IP-Eigenschaften der jeweiligen Verbindung (LAN oder DFÜ).

F: Ich entdecke weder Anti Spam, SurfControl noch Anti Spam und SurfControl. Was kann ich tun?

A: In dem Fall verwenden Sie den falschen Registrierungsschlüssel. Bitte bestellen Sie über die Software auf der Statusseite den geeigneten Registrierungsschlüssel.

F: Nach der Installation ist der PC extrem langsam. Programme öffnen sich erst nach extrem langer Zeit. Was kann ich tun?

A: In der Regel deutet dieses Verhalten auf einen Mangel an Arbeitsspeicher (RAM) hin. Dieser wird vom Echtzeitschutz benötigt. Der Echtzeitschutz prüft jede Datei vor der Ausführung auf evtl. enthaltene Infektionen. Dazu ist ein gewisser Bereich des RAMs freizuhalten, damit die zu scannende Datei in diesen geladen werden kann. Sollte Ihr PC nicht über ausreichend RAM verfügen, können Sie den Echtzeitschutz auf einen Bereich kritischer Dateiendungen eingrenzen. Zu den kritischen Dateiendungen gehören z. B. Dateien, die auf .EXE, .BAT oder .SYS enden. Zur Konfiguration des Echtzeitschutzes schauen Sie bitte im Handbuch unter 4.5.1 Echtzeit Scanning auf Seite 44 nach.

Virenschutz

F: Bei der Installation von Software mit großen Datenmengen wird man aufgefordert, den Virenscanner für die Zeit der Installation abzuschalten – ist das nicht gefährlich?

A: Wir empfehlen, vor Beginn der Installation einen manuellen Scan der Installationssoftware durchzuführen, um die Virenfreiheit festzustellen. Für die Zeit der Installation sollte der Echtzeitschutz ausgeschaltet werden. Es ist nicht erforderlich, den kompletten Virenschutz zu deaktivieren.

F: Ich kann einige Programme nicht installieren, weil die Virenschutzanwendung meldet, dass sie von einem Virus infiziert worden sind. Was ist zu tun?

A: Wenn die Virenschutzanwendung einen Virus identifiziert, d. h. den Namen eines Virus meldet, sollten Sie die Installation nicht fortsetzen. Wenn kein Virus namentlich genannt wird, haben Sie wahrscheinlich das strengste Profil für den Virenschutz aktiviert, und der heuristische Scanner hat ein vergleichbares Verhalten er-

kannt, ähnlich wie bei einer Virusinfektion. In diesem Fall wenden Sie sich bitte an den Support. Dieser wird durch die Firma F-Secure die bemängelte Datei prüfen lassen, um die Virenfreiheit feststellen zu können.

Virenscan

F: Personal Security Service kann eine infizierte Datei auf dem Computer nicht desinfizieren, löschen oder umbenennen. Was soll ich tun?

A: Siehe Abschnitt **Viren nach Fehlschlagen des Desinfektions-Assistenten entfernen** auf Seite 41.

F: Nach dem Virenscan wird mir gesagt, dass sich eine Infektion im Verzeichnis C:\Windows\Restore befindet, die nicht desinfiziert, umbenannt oder gelöscht werden konnte. Ich habe auch keine Möglichkeit, diese Datei manuell zu löschen. Was soll ich tun?

A: Das Restore-Verzeichnis gibt es nur bei Windows ME und Windows XP. Es wird automatisch durch das Betriebssystem angelegt, sobald die Systemwiederherstellung aktiviert wird. Da ausschließlich das System auf diesen Ordner zugreifen kann, ist es PSS nicht möglich, die Dateien in dem Ordner zu behandeln. Es fehlen die Schreibrechte für die Dateien. Sollte eine Infektion in diesem Ordner enthalten sein, gehen Sie bitte wie folgt vor:

Windows XP:

- Wählen Sie mit einem Rechtsklick **Mein Computer** aus.
- Wählen Sie **Eigenschaften.**
- Wählen Sie **Systemwiederherstellung**.
- Wählen Sie **Systemwiederherstellung deaktivieren.**
- Drücken Sie den Button **Anwenden.**
- Klicken Sie auf **OK.**
- Führen Sie einen Neustart des Rechners durch.

Windows ME:

- Schließen Sie alle geöffneten Programme.
- Wählen Sie mit einem Rechtsklick **Mein Computer** aus.
- Wählen Sie **Eigenschaften.**
- Wählen Sie **Performance.**

- Wählen Sie **Dateisysteme** aus.
- Wählen Sie **Fehlersuche.**
- Deaktivieren Sie die **System Wiederherstellung**.
- Klicken Sie auf **OK.**
- Klicken Sie auf **Schließen.**
- Führen Sie einen Neustart des Rechners durch.

In beiden Fällen sollte nun das Restore-Verzeichnis automatisch gelöscht sein und damit auch alle enthaltenen Infektionen. Zur Sicherheit scannen Sie bitte erneut die komplette Festplatte. Anschließend können Sie die Systemwiederherstellung wieder aktivieren.

Dialerschutz-Funktion

F: Die Wählverbindung zu meinem Internet-Service-Provider (oder zu einer anderen Rufnummer) kann nicht hergestellt werden. Was soll ich tun?

A: Möglicherweise haben Sie versehentlich die Verbindung zu Ihrem Internet-Service-Provider abgelehnt. Lesen Sie mehr über das Zulassen von Verbindungen im Kapitel **5.7 Dialerschutz** auf Seite 78. Überprüfen Sie alle Rufnummerneinträge in der Rufnummernliste des Dialerschutzes, bei denen Sie einen Platzhalter („?“ oder „X“) eingegeben haben. Allerdings kann es auch sein, dass die bestehende Verbindung zum Internet-Service-Provider abgebrochen wird, weil ein Dialerprogramm eine Verbindung aufbauen möchte. Auch wenn Sie die Verbindung zu dem bösartigen Dialer abgelehnt haben, versucht der Dialer, eine DFÜ-Verbindung aufzubauen, und wird durch Personal Security Service daran gehindert. In dem Fall ist es notwendig, dass Sie eine neue Verbindung zu Ihrem Internet-Service-Provider aufbauen.

F: In der Rufnummernliste befindet sich eine vordefinierte Rufnummer, die z. B. lautet „Lehne 0190X ab“. Wie kann ich diesen Eintrag löschen?

A: Dieser Rufnummerneintrag verhindert alle Verbindungen zu Rufnummern, die mit 0190 beginnen. Die einzige Möglichkeit, diese Rufnummer zu ändern, ist, eine neue Regel hinzuzufügen, um die Verbindung zu dieser Rufnummer zu erlauben und diesen Eintrag über die ursprüngliche Regel zu verschieben. Weitere Informationen dazu finden Sie im Kapitel **5.7 Dialerschutz** auf Seite 78.

F: Ein auf meinem Computer befindliches Dialerprogramm beeinträchtigt die Prozessorleistung meines Computers. Was kann ich tun?

A: Bitte löschen Sie alle Dialerprogramme von Ihrem Computer. Ein auf einem Computer befindliches Dialerprogramm versucht, immer wieder eine DFÜ-Verbindung aufzubauen, und die Dialerschutz-Funktion unterbindet jeden Verbindungswunsch, sofern Sie den Dialer abgelehnt haben. Diese Aktionen belasten die Leistungsfähigkeit Ihres Prozessors. So kann es dazu kommen, dass andere Anwendungen nur sehr zeitverzögert arbeiten oder im schlimmsten Fall gar nicht mehr reagieren, solange diese Dialerprogramme nicht gelöscht wurden. Falls Sie dabei unsere Unterstützung benötigen, stehen wir Ihnen gerne zur Verfügung. Bitte wenden Sie sich an die Mitarbeiter des Hotline-Supports unter 0800 8 35 37 32 (1,79 € pro Minute).

Internet-Schutzschild

F: Die Software meldet eine Funktionsstörung in der Firewall. Was ist zu tun?

A: In der Regel deuten Funktionsstörungen darauf hin, dass entweder noch eine andere Firewallkomponente auf dem PC installiert ist oder die Systemressourcen nicht zum Betrieb der Software ausreichen. Im ersten Fall deinstallieren Sie alle Fragmente der Firewall des Drittanbieters. Im zweiten Fall rüsten Sie Ihren PC auf (RAM oder Prozessor).

Anwendungssteuerung

F: Wie kann ich die Berechtigungen der Anwendung für Internetverbindungen ändern? Wie kann ich für eine Anwendung, für die dies bisher untersagt war, Internetverbindungen zulassen?

A: Siehe Abschnitt **5.5.1 Anwendungseigenschaften** auf Seite 70 im Handbuch.

F: Mein E-Mail-Programm (bzw. ein anderes Programm wie beispielsweise der Internet-Browser) funktioniert nicht mehr.

A: Sie haben unter Umständen versehentlich eingestellt, dass das Programm keine Verbindungen herstellen darf. Weitere Informationen zum Zulassen von Verbindungen finden Sie im Abschnitt **5.5.1 Anwendungseigenschaften** auf Seite 70 im Handbuch.

F: Für welche Programme bzw. Anwendungen können Verbindungen zum Internet zugelassen werden?

A: Weitere Informationen zur Bestimmung, für welche Anwendungen Verbindungen verhindert oder zugelassen werden sollen, finden Sie im Abschnitt **5.5.1 Anwendungseigenschaften** auf Seite 70 im Handbuch.

SurfControl

F: Ich habe mein Passwort vergessen, was kann ich tun?

A: Wenn Sie Ihr Passwort vergessen haben, können Sie es durch die Eingabe Ihres Registrierungsschlüssels zurücksetzen. Sie können das Passwort über die erweiterten Einstellungen von SurfControl ändern.

F: Ich möchte SurfControl deaktivieren, wenn ich am Computer arbeite. Wie soll ich vorgehen?

A: Wenn Sie SurfControl vorübergehend deaktivieren möchten, wählen Sie über das Taskleisten-Symbol neben der Uhranzeige mit der rechten Maustaste den Befehl **Webseitenfilter aussetzen,** oder klicken Sie im Microsoft Internet Explorer auf die Symbolleistenschaltfläche **SurfControl.** SurfControl ist bei einer vorübergehenden Aussetzung nur während der aktuellen Sitzung ausgeschaltet. Sobald sich ein anderer Teilnehmer bei Windows anmeldet, wird die Funktion automatisch wieder gestartet. Wenn Sie SurfControl über die Benutzeroberfläche deaktivieren, werden alle Funktionen von SurfControl dauerhaft ausgeschaltet, bis Sie sie wieder aktivieren.

F: Mein Webseitenfilter ist aktiviert, aber dennoch werden Inhalte angezeigt, die nach Auswahl der Filterkategorien nicht angezeigt werden sollen. Was stimmt nicht?

A: Falls es sich bei diesen Webseiten nicht um HTTP-Webseiten, sondern um HTTPS-Webseiten handelt, kann der Inhalt auf Grund der Verschlüsselung von SurfControl nicht überprüft werden. Falls dieser Fall bei Ihnen nicht zutrifft, senden Sie uns eine E-Mail mit der URL (Adresse der Webseite) zu.

F: Ist mein Computer auch vor neuen Dialer-Typen geschützt?

A: Ihr Computer ist vor allen gegenwärtig bekannten Dialer-Techniken geschützt.

F: Die Festplatten meines Computers sind in viele Partitionen aufgeteilt. Kann ich unbesorgt jede Partition verwenden, um online zu gehen?

A: Ja, das können Sie. Unabhängig von der verwendeten Partition fängt der Dialerschutz DFÜ-Verbindungsversuche ab.

Automatische Updates

F: Was passiert, wenn mein Computer bei Fälligkeit einer automatischen Virendefinitions-Datenbank-Aktualisierung offline ist?

A: Wenn Sie das nächste Mal online sind, lädt Personal Security Service die aktuellste Virendefinitions-Datenbank-Aktualisierung automatisch herunter.

F: Wie oft sollte die Virendefinitions-Datenbank aktualisiert werden?

A: Virendefinitions-Datenbanken werden automatisch aktualisiert, wenn die Funktion zur automatischen Aktualisierung aktiviert ist. Wenn Sie die Datenbanken manuell aktualisieren möchten, sollten Sie dies mehrmals wöchentlich (am besten täglich) vornehmen.

F: Ich versuche, manuell nach Virendefinitions-Datenbank-Aktualisierungen zu suchen (durch Klicken auf „Jetzt prüfen“), aber nichts passiert.

A: Wenn Sie ein Modem verwenden oder über einen ISDN-Anschluss verfügen, müssen Sie vor dem Klicken auf **Jetzt prüfen** manuell eine Verbindung zum Internet herstellen. Falls selbst dann keine Prüfung nach neuen Updates stattfindet, schauen Sie bitte in der Protokolldatei nach evtl. Fehlermeldungen. Im Zweifel kontaktieren Sie unseren Support.

Anti Spam

F: Obwohl Anti Spam aktiviert ist, finde ich weiterhin Massen-E-Mails in meinem Posteingang. Wie lässt sich dieses Problem beheben?

A: Vergewissern Sie sich, dass Ihr E-Mail-Client ordnungsgemäß für eine Zusammenarbeit mit Anti Spam eingerichtet wurde. Ändern Sie auf der Seite mit den erweiterten Einstellungen für Anti Spam die Filterstufe, um mehr Nachrichten als Spam zu filtern.

F: Ich nutze den T-Online E-Mail-Client und es lässt sich kein Spam-Ordner erstellen. Was muss ich tun?

A: Da der T-Online Client es nicht zulässt, eigene Regeln für die Betreffzeile zu definieren, kann hierbei kein Spam-Ordner angelegt werden. Hier besteht nur die Möglichkeit, einen anderen E-Mail-Client zu nutzen, z. B. Outlook Express.

Glossar

Anwendung. Ein für einen bestimmten Zweck geschriebenes Software-Programm. Anwendungen sind in der Regel manuell zu starten.

Anwendungssteuerung. Die Anwendungssteuerung ist eine Funktion in Personal Security Service, mit der eine Anwendung, die von Ihrem Computer aus mit dem Internet verbunden ist, automatisch geprüft wird, indem die Anwendung mit der Liste von sicheren (bereits genehmigten) Software-Programmen und bereits als schädlich bekannten Software-Programmen (Trojaner usw.) verglichen wird.

Denial-of-Service-Angriffe. Ein expliziter Angriffsversuch, bei dem berechtigte Benutzer durch Unterbrechung der Verbindungen, Überlastung eines Netzwerks oder Unterbinden des Netzwerkzugriffs einzelner Personen an der Verwendung eines Dienstes gehindert werden.

Dialer. Dialer sind Programme (EXE-Dateien), die auf dem Rechner einen neuen Internet-Zugang einrichten. Nach dem Download und der Installation auf dem PC wählt sich der Dialer über das Modem oder die ISDN-Karte ins Internet ein. Eine zu dieser Zeit bereits bestehende Internetverbindung wird in der Regel zuvor getrennt. Die Zugangsnummer, die der Dialer bei der neuen Einwahl benutzt, bestimmt die Höhe der anfallenden Kosten. Dialer funktionieren in aller Regel nur auf dem Betriebssystem Windows. Dies liegt an der marktbeherrschenden Position des Microsoft-Betriebssystems; offenbar lohnt es sich für Dialeranbieter bislang nicht, Dialer auch für andere Betriebssysteme zu entwickeln.

DNS. Im Domänennamensystem (DNS) sind die Namen der Internet-Domäne enthalten und in Internet-Protokolladressen übersetzt. Ein Domänenname ist eine aussagekräftige, leicht merkbare Beschreibung für eine Internet-Adresse. Die Internet-Adresse www.some.domain.org ist beispielsweise ein DNS-Name.

Heuristisch. Untersuchende Problemlösung, bei der selbst lernende Techniken angewandt werden.

Hotfix. Datenpaket zur Behebung eines Softwarefehlers.

Malware (schädliche Programme). Schädliche Programme, so genannte „Malware“, sind Programme oder Dateien, die eigens dafür entwickelt wurden, um Schaden anzurichten.

Paket. Ein Paket ist eine Dateneinheit, die von einer Quelle zu einem Ziel im Internet gesendet wird. Wenn Dateien (z. B. eine E-Mail) im Internet von einer Adresse zur anderen gesendet werden, werden diese in passende Pakete aufgeteilt und gesendet. Wenn sie ihren Adressaten erreicht haben, werden sie wieder zur ursprünglichen Datei zusammengesetzt.

Schädliche Programme. Schädliche Programme, so genannte „Malware“, sind Programme oder Dateien, die allein dazu entwickelt wurden, auf Ihrem Computer Schaden anzurichten. Dazu gehören Computerviren, Würmer und Trojanische Pferde.

Schutzstufe. Schutzstufen sind im Voraus konfigurierte Sicherheitseinstellungen, mit denen Ihre Sicherheitsstufe festgelegt wird. Sie werden automatisch aktualisiert, damit Sie jederzeit gegen neue Arten bösartiger Computerprogramme und Internet-Angriffe geschützt sind.

Spam. Bei Spam-Nachrichten handelt es sich um in großen Mengen versandte Werbemails an Personen, die diese Mails normalerweise nicht erhalten möchten.

Teilnetz. Dieser Begriff steht für Teilnetzwerk, d. h. bildet einen Abschnitt eines Netzwerks. Computer mit demselben Teilnetz sind sich in der Regel physisch nahe und verfügen über IP-Adressen, deren erste zwei oder drei Ziffern identisch sind.

Trojanisches Pferd. Ein Programm, das absichtlich Aktionen durchführt, die der Benutzer des Programms nicht erwartet.

Virendefinitions-Datenbank. Mit Virendefinitions-Datenbanken werden Viren entdeckt. Wenn ein neuer Virus entdeckt wird, müssen die Datenbanken aktualisiert werden, damit der Virenschutz diesen Virus ermitteln kann.

Virus. Ein Computerprogramm, das sich durch eigene Reproduktion verbreitet.

Wurm. Ein Computerprogramm, das sich selbst durch Einfügen eigener Kopien in Netzwerk-Computern vermehren kann.

Technische Unterstützung

Kunden mit der Vollversion können sich bei Fragen zur Installation oder zum Betrieb der Software an die Mitarbeiter des Hotline-Supports unter 0800 8 35 37 32 (pro Minute wird 1,79 € nach erfolgter Verbindung zu einem Mitarbeiter des Second-Level-Supports in Rechnung gestellt; die Kosten werden lediglich für die Beratung berechnet, jedoch nicht für die Verbindung selbst) wenden, der montags bis freitags von 8.00 bis 20.00 Uhr und samstags von 8.00 bis 16.00 Uhr zur Verfügung steht. Um Ihnen schnellstmöglich Unterstützung anbieten zu können, halten Sie bitte Ihre Kundennummer bereit. Diese finden Sie in Ihrer Telefonrechnung.

Darüber hinaus können Sie Ihre Frage auch über ein Webformular an unseren Support senden.

Bitte verwenden Sie das Webformular unter
https://pss.t-com.de/support/email_support.html

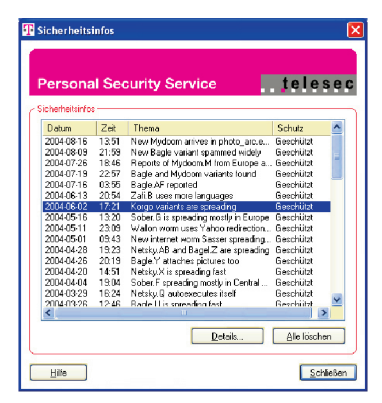
Für Kunden der Testversion und Vollversion halten wir unter
http://www.t-com.de/pss-faq eine Liste mit Antworten zu den
am häufigsten gestellten Fragen (FAQ) bereit.

Besuchen Sie auch die Produktseite Personal Security Service unter
www.t-com.de/pss. Dort finden Sie weitere aktuelle Informationen zu
Personal Security Service.

Wartung

Virendefinitions-Datenbanken werden während des Anmeldezeitraums automatisch auf Ihrem Computer aktualisiert. Während der Zeit Ihrer Anmeldung werden Ihnen bei Bedarf von Zeit zu Zeit zusätzlich und kostenfrei neue Software-Versionen, Dienstpakete und „Hotfixes“ zur Verfügung gestellt. Eine umfangreiche Sammlung an aktuellen, virenbezogenen Informationen und Beschreibungen finden Sie neuerdings auf unserer Webseite www.t-com.de/vireninfokatalog in Deutsch vor. Bis die Übersetzung verfügbar ist, finden Sie vorerst die englische Beschreibung vor.

Außerdem haben Sie mit der Version 5.0 die Möglichkeit, über die Software selbst Virennachrichten zu einem späteren Zeitpunkt noch mal aufzurufen. Klicken Sie dazu auf Homepage. Im Anschluss daran klicken Sie bitte auf Ansicht neben den Sicherheitsinfos.



Herausgeber:
Deutsche Telekom AG,
T-Com Zentrale
Postfach 20 00
53105 Bonn

Weitere Informationen im T-Punkt Business, unter freecall 0800 33 01300* oder www.t-com.de/pss

* Allgemeine Infos zum Produkt sind kostenlos, die Weiterleitung zum technischen Support für Fragen zur Installation oder zum Betrieb der Software ist kostenpflichtig (1,79 €/Min. brutto).

